# CYBER SECURITY PRO

## FÜR MAC

Benutzerhandbuch

(für Produktversion 6.0 und höher)

Klicken Sie hier, um die aktuelle Version dieses Dokuments herunterzuladen.

© **ESET, spol. s r.o.**
ESET Cyber Security Pro wurde entwickelt von ESET, spol. s r.o.
Weitere Informationen finden Sie auf www.eset.com.
Alle Rechte vorbehalten. Kein Teil dieser Dokumentation darf ohne schriftliche Einwilligung des Verfassers reproduziert, in einem Abrufsystem gespeichert oder in irgendeiner Form oder auf irgendeine Weise weitergegeben werden, sei es elektronisch, mechanisch, durch Fotokopien, Aufnehmen, Scannen oder auf andere Art.
ESET, spol. s r.o. behält sich das Recht vor, ohne vorherige Ankündigung an jedem der hier beschriebenen Software-Produkte Änderungen vorzunehmen.

Support: www.eset.com/support

REV. 24/06/2014

# Inhalt


1. ESET Cyber Security Pro ..... 4
1.1 Neuerungen ..... 4
1.2 Systemanforderungen ..... 4
2. Installation ..... 4
2.1 Standardinstallation ..... 4
2.2 Benutzerdefinierte Installation ..... 5
3. Produktaktivierung ..... 5
4. Deinstallation ..... 6
5. Übersicht ..... 6
5.1 Tastaturbefehle ..... 6
5.2 Schutzstatus prüfen ..... 6
5.3 Vorgehensweise bei fehlerhafter Ausführung des Programms ..... 6
6. Computerschutz ..... 7
6.1 Viren- und Spyware-Schutz ..... 7
6.1.1 Allgemein ..... 7
6.1.1.1 Ausschlussfilter ..... 7
6.1.2 Systemstart-Schutz ..... 7
6.1.3 Echtzeit-Dateischutz ..... 7
6.1.3.1 Prüfen beim (Prüfen bei Ereignis) ..... 8
6.1.3.2 Erweiterte Einstellungen ..... 8
6.1.3.3 Wann sollten die Einstellungen für den Echtzeit-Dateischutz geändert werden? ..... 8
6.1.3.4 Echtzeit-Dateischutz prüfen ..... 8
6.1.3.5 Vorgehensweise bei fehlerhaftem Echtzeit-Dateischutz ..... 8
6.1.4 On-Demand-Prüfung ..... 8
6.1.4.1 Prüfungstyp ..... 9
6.1.4.1.1 Smart-Prüfung ..... 9
6.1.4.1.2 Prüfen mit speziellen Einstellungen ..... 9
6.1.4.2 Zu prüfende Objekte ..... 9
6.1.4.3 Prüfprofile ..... 9
6.1.5 ThreatSense-Einstellungen ..... 10
6.1.5.1 Objekte ..... 10
6.1.5.2 Optionen ..... 10
6.1.5.3 Säubern ..... 10
6.1.5.4 Erweiterungen ..... 11
6.1.5.5 Grenzen ..... 11
6.1.5.6 Sonstige ..... 11
6.1.6 Eingedrungene Schadsoftware wurde erkannt ..... 11
6.2 Prüfen und Sperren von Wechselmedien ..... 12
7. Phishing-Schutz ..... 12
8. Firewall ..... 12
8.1 Filtermodi ..... 12
8.2 Firewall-Regeln ..... 13
8.2.1 Erstellen neuer Regeln ..... 13
8.3 Firewall-Zonen ..... 13
8.4 Firewall-Profile ..... 13
8.5 Firewall-Logs ..... 14
9. Web- und E-Mail-Schutz ..... 14
9.1 Web-Schutz ..... 14
9.1.1 Ports ..... 14
9.1.2 Aktiver Modus ..... 14
9.1.3 URL-Listen ..... 14
9.2 E-Mail-Schutz ..... 14
9.2.1 Prüfen von E-Mails per POP3-Protokoll ..... 15
9.2.2 Prüfen von E-Mails per IMAP-Protokoll ..... 15
10. Kindersicherung ..... 15
11. Update ..... 16
11.1 Einstellungen für Updates ..... 16
11.2 So erstellen Sie Update-Tasks ..... 16
11.3 Upgrade von ESET Cyber Security Pro auf eine neue Version ..... 16
11.4 Systemupdates ..... 17
12. Tools ..... 17
12.1 Log-Dateien ..... 17
12.1.1 Log-Wartung ..... 17
12.1.2 Log-Filter ..... 18
12.2 Taskplaner ..... 18
12.2.1 Erstellen von Tasks ..... 18
12.2.2 Erstellen von benutzerdefinierten Tasks ..... 18
12.3 Quarantäne ..... 19
12.3.1 Quarantäne für Dateien ..... 19
12.3.2 Wiederherstellen aus Quarantäne ..... 19
12.3.3 Einreichen von Dateien aus der Quarantäne ..... 19
12.4 Ausgeführte Prozesse ..... 19
12.5 Live Grid ..... 20
12.5.1 Live Grid-Einstellungen ..... 20
12.6 ESET Social Media Scanner ..... 20
13. Benutzeroberfläche ..... 20
13.1 Warnungen und Hinweise ..... 21
13.1.1 Erweiterte Einstellungen für Warnungen und Hinweise ..... 21
13.2 Berechtigungen ..... 21
13.3 Kontextmenü ..... 21
14. Allgemein ..... 22
14.1 Einstellungen importieren/exportieren ..... 22
14.1.1 Einstellungen importieren ..... 22
14.1.2 Einstellungen exportieren ..... 22
14.2 Einstellungen für Proxyserver ..... 22
15. Glossar ..... 22
15.1 Arten von Infiltrationen ..... 22
15.1.1 Viren ..... 22
15.1.2 Würmer ..... 23
15.1.3 Trojaner ..... 23
15.1.4 Rootkits ..... 23
15.1.5 Adware ..... 23
15.1.6 Spyware ..... 23
15.1.7 Potenziell unsichere Anwendungen ..... 24
15.1.8 Evtl. unerwünschte Anwendungen ..... 24
15.2 Arten von Remote-Angriffen ..... 24
15.2.1 DoS-Angriffe ..... 24
15.2.2 DNS Poisoning ..... 24
15.2.3 Portscans ..... 24
15.2.4 TCP Desynchronisation ..... 24
15.2.5 SMB Relay ..... 25
15.2.6 ICMP-Angriffe ..... 25
15.3 E-Mail ..... 25
15.3.1 Werbung ..... 25
15.3.2 Hoaxes ..... 26
15.3.3 Phishing ..... 26
15.3.4 Erkennen von Spam ..... 26

# 1. ESET Cyber Security Pro

ESET Cyber Security Pro stellt eine neue Herangehensweise an integrierte Computersicherheit dar. Die aktuelle Version des ThreatSense®-Prüfmoduls bietet in Kombination mit dem E-Mail-Client-Schutz, der Personal Firewall und einer Kindersicherung schnellen, präzisen Schutz für Ihren Computer. Das Ergebnis ist ein intelligentes System, das Ihren Computer fortwährend auf externe Angriffe und das Eindringen von Schadsoftware überwacht.

ESET Cyber Security Pro ist als umfassende Sicherheitslösung das Ergebnis unserer langjährigen Entwicklungsarbeit für maximalen Schutz bei minimaler Systembelastung. Seine auf künstlicher Intelligenz basierenden, zukunftsweisenden Technologien sind in der Lage, das Eindringen von Viren, Würmern, Trojanern, Spyware, Adware und Rootkits sowie andere Angriffe aus dem Internet proaktiv zu verhindern, ohne die Systemleistung zu beeinträchtigen oder den Betrieb Ihres Computers zu stören.

## 1.1 Neuerungen

Im Vergleich zu ESET Cyber Security Pro Version 5 wurden in Version 6 folgende Neuerungen und Verbesserungen eingeführt:

**Phishing-Schutz**
Verhindert, dass als vertrauenswürdig getarnte Websites auf Ihre persönlichen Informationen zugreifen.

**Integration von ESET Social Media Scanner**
ESET Cyber Security Pro kann mit einer Anwendung verknüpft werden, die Ihre Facebook- und Twitter-Konten vor Bedrohungen schützt. Die Anwendung ist unabhängig von anderen ESET-Produkten und völlig kostenlos.

**Systemupdates**
ESET Cyber Security Pro Version 6 enthält verschiedene Korrekturen und Verbesserungen, unter anderem eine Benachrichtigungsfunktion für Betriebssystemupdates unter Mac OS X 10.8. Weitere Informationen hierzu finden Sie im Abschnitt Systemupdates 17.

## 1.2 Systemanforderungen

Um mit ESET Cyber Security Pro eine optimale Leistung zu erreichen, sollten die folgenden Hardware- und Softwareanforderungen erfüllt sein:

| | Systemanforderungen |
|---|---|
| Prozessorarchitektur | Intel® Prozessor mit 32/64 Bit |
| Betriebssystem | Mac OS X 10.6 oder höher |
| Arbeitsspeicher | 300 MB |
| Freier Speicher | 150 MB |

# 2. Installation

Bitte schließen Sie alle laufenden Programme, bevor Sie mit der Installation beginnen. ESET Cyber Security Pro enthält Komponenten, durch die es zu Konflikten mit anderen Virenschutzprogrammen auf Ihrem Computer kommen kann. ESET empfiehlt daher dringend, alle anderen Virenschutzprogramme zu deinstallieren, um Probleme zu vermeiden.

Führen Sie einen der folgenden Schritte aus, um den Installationsassistenten zu starten:

- Bei der Installation per CD/DVD legen Sie diese in Ihren Computer ein, öffnen Sie sie über den Desktop oder ein **Finder**-Fenster und doppelklicken Sie auf das Symbol **Installieren**.
- Wenn Sie zur Installation eine Datei verwenden, die Sie von der ESET-Website heruntergeladen haben, öffnen Sie diese und doppelklicken Sie auf das Symbol **Installieren**.

Der Installationsassistent führt Sie durch die grundlegende Einrichtung. Zu Beginn der Installation prüft das Installationsprogramm automatisch online auf die neueste Produktversion. Wird eine neuere Version gefunden, erhalten Sie die Möglichkeit, vor dem Fortsetzen der Installation die neueste Version herunterzuladen.

Nachdem Sie der Endbenutzer-Lizenzvereinbarung zugestimmt haben, werden Sie aufgefordert, eine der folgenden Installationsarten auszuwählen:

- Standardinstallation 4
- Benutzerdefinierte Installation 5

## 2.1 Standardinstallation

Bei der Standardinstallation wird eine Konfiguration verwendet, die für die Anforderungen der meisten Benutzer geeignet ist. Sie bietet optimale Sicherheit und gleichzeitig gute Systemleistung. Die Standardinstallation wird daher empfohlen, wenn Sie keine speziellen Anforderungen an die Konfiguration haben.

**Live Grid**
Durch das Live Grid-Frühwarnsystem ist ESET beim Auftauchen neuer Infiltrationen immer auf dem neuesten Stand und kann seine Kunden schneller schützen. Neue Bedrohungen werden zur Analyse und Verarbeitung an das ESET-Virenlabor übermittelt und dann zur Signaturdatenbank hinzugefügt. Standardmäßig ist die Option **Live Grid-Frühwarnsystem aktivieren** aktiviert. Wenn Sie genauere Einstellungen für die Übermittlung verdächtiger Dateien vornehmen möchten, klicken Sie auf **Einstellungen**. Weitere Informationen finden Sie im Abschnitt Live Grid 20.

**Sonderanwendungen**
Im letzten Schritt der Installation wird die Prüfung auf **Evtl. unerwünschte Anwendungen** konfiguriert. Bei eventuell unerwünschten Anwendungen handelt es sich um Programme, die zwar nicht unbedingt Sicherheitsrisiken in sich bergen, jedoch negative Auswirkungen auf das Verhalten Ihres

Computers haben können. Diese Anwendungen sind oft mit anderen Programmen gebündelt und daher während des Installationsvorgangs schwer erkennbar. Obwohl bei solchen Anwendungen während der Installation gewöhnlich eine Benachrichtigung angezeigt wird, können sie auch leicht ohne Ihre Zustimmung installiert werden.

Nach der Installation von ESET Cyber Security Pro sollte der Computer auf Schadcode geprüft werden. Klicken Sie dazu im Hauptprogrammfenster auf **Computer prüfen** und dann auf **Smart-Prüfung**. Nähere Informationen zur On-Demand-Prüfung finden Sie im Abschnitt On-Demand-Prüfung 8.

### 2.2 Benutzerdefinierte Installation

Die benutzerdefinierte Installation eignet sich für fortgeschrittene Benutzer, die während der Installation die erweiterten Einstellungen ändern möchten.

**Proxyserver**
Wenn Sie einen Proxyserver verwenden, können Sie jetzt die entsprechenden Parameter festlegen. Wählen Sie dazu die Option **Ich nutze einen Proxyserver**. Geben Sie im nächsten Schritt unter **Adresse** die IP-Adresse oder URL des Proxyservers ein. Geben Sie dann im Feld **Port** den Port an, über den Verbindungen auf dem Proxyserver eingehen (standardmäßig 3128). Falls für den Proxyserver Zugangsdaten zur Authentifizierung erforderlich sind, geben Sie einen gültigen **Benutzernamen** und das **Passwort** ein. Wenn Sie sicher sind, dass Sie keinen Proxyserver verwenden, wählen Sie die Option **Keinen Proxyserver verwenden**. Wenn Sie unsicher sind, können Sie Ihre aktuellen Systemeinstellungen verwenden. Wählen Sie dazu **Systemeinstellungen verwenden (empfohlen)**.

**Berechtigungen**
Im nächsten Schritt können Sie privilegierte Benutzer definieren, die berechtigt sind, die Programmkonfiguration zu ändern. Wählen Sie aus der Liste links die Benutzer aus und fügen Sie sie über die Schaltfläche **Hinzufügen** zur Liste **Privilegierte Benutzer** hinzu. Um alle Systembenutzer anzuzeigen, wählen Sie die Option **Alle Benutzer anzeigen**. Wenn Sie die Liste der privilegierten Benutzer leer lassen, werden alle Benutzer als privilegiert betrachtet.

**Live Grid**
Durch das Live Grid-Frühwarnsystem ist ESET beim Auftauchen neuer Infiltrationen immer auf dem neuesten Stand und kann seine Kunden schneller schützen. Neue Bedrohungen werden zur Analyse und Verarbeitung an das ESET-Virenlabor übermittelt und dann zur Signaturdatenbank hinzugefügt. Standardmäßig ist die Option **Live Grid-Frühwarnsystem aktivieren** aktiviert. Wenn Sie genauere Einstellungen für die Übermittlung verdächtiger Dateien vornehmen möchten, klicken Sie auf **Einstellungen**. Weitere Informationen finden Sie im Abschnitt Live Grid 20.

**Sonderanwendungen**
Im nächsten Schritt der Installation wird die Prüfung auf **Evtl. unerwünschte Anwendungen** konfiguriert. Bei eventuell unerwünschten Anwendungen handelt es sich um Programme, die zwar nicht unbedingt Sicherheitsrisiken in sich bergen, jedoch negative Auswirkungen auf das Verhalten Ihres Computers haben können. Diese Anwendungen sind oft mit anderen Programmen gebündelt und daher während des Installationsvorgangs schwer erkennbar. Obwohl bei solchen Anwendungen während der Installation gewöhnlich eine Benachrichtigung angezeigt wird, können sie auch leicht ohne Ihre Zustimmung installiert werden.

**Personal Firewall: Filtermodus**
Im letzten Schritt können Sie einen Filtermodus für die Personal Firewall auswählen. Weitere Informationen finden Sie unter Filtermodi 12.

Nach der Installation von ESET Cyber Security Pro sollte der Computer auf Schadcode geprüft werden. Klicken Sie dazu im Hauptprogrammfenster auf **Computer prüfen** und dann auf **Smart-Prüfung**. Nähere Informationen zur On-Demand-Prüfung finden Sie im Abschnitt On-Demand-Prüfung 8.

## 3. Produktaktivierung

Nach der Installation wird das Fenster **Art der Produktaktivierung** automatisch auf Ihrem Bildschirm angezeigt. Alternativ können Sie auf das ESET Cyber Security Pro-Symbol oben in der Menüleiste und dann auf **Produktaktivierung** klicken.

1. Wenn Sie das Produkt im Einzelhandel gekauft haben, wählen Sie die Option **Aktivierung mithilfe eines Aktivierungsschlüssels**. Den Aktivierungsschlüssel finden Sie üblicherweise im Inneren oder auf der Rückseite der Produktverpackung. Zur erfolgreichen Aktivierung müssen Sie den Aktivierungsschlüssel genau wie angegeben eingeben.

2. Wenn Sie einen Benutzernamen und ein Passwort erhalten haben, aktivieren Sie die Option **Aktivierung mithilfe eines Benutzernamens und eines Passworts** und geben Sie die Lizenzdaten in die entsprechenden Felder ein. Diese Option ist entspricht der Option **Lizenzdaten eingeben** im Fenster **Update**.

3. Wenn Sie ESET Cyber Security Pro vor dem Kauf erst einmal testen möchten, wählen Sie die Option **Testlizenz aktivieren** . Geben Sie Ihre E-Mail-Adresse an, um ESET Cyber Security Pro für einen begrenzten Zeitraum zu aktivieren. Ihre Testlizenz wird Ihnen per E-Mail zugeschickt. Eine Testlizenz kann pro Kunde nur ein einziges Mal aktiviert werden.

Wenn Sie die Aktivierung zu einem späteren Zeitpunkt vornehmen möchten, klicken Sie auf **Später aktivieren**. Sie können ESET Cyber Security Pro direkt über die **Startseite** oder über den Abschnitt **Update** im Hauptprogrammfenster von ESET Cyber Security Pro aktivieren.

Wenn Sie noch keine Lizenz besitzen und gern eine kaufen möchten, klicken Sie auf die Option **Lizenz**. Hiermit gelangen Sie zur Website Ihres örtlichen ESET-Vetriebshändlers.

# 4. Deinstallation

Zur Deinstallation von ESET Cyber Security Pro wählen Sie eine der folgenden Methoden:

- Legen Sie die Installations-CD/-DVD von ESET Cyber Security Pro in Ihren Computer ein, öffnen Sie sie über den Desktop oder ein **Finder**-Fenster und doppelklicken Sie auf das Symbol **Deinstallieren**.
- Öffnen Sie die Installationsdatei von ESET Cyber Security Pro (*DMG*-Datei) und doppelklicken Sie auf das Symbol **Deinstallieren**.
- Öffnen Sie im **Finder** den Ordner **Programme** auf Ihrer Festplatte, halten Sie die Ctrl-Taste gedrückt, klicken Sie auf das Symbol von **ESET Cyber Security Pro** und wählen Sie Option **Paketinhalt zeigen**. Öffnen Sie den Ordner **Resources** und doppelklicken Sie auf das Symbol zur **Deinstallation**.

# 5. Übersicht

Das Hauptprogrammfenster von ESET Cyber Security Pro ist in zwei Abschnitte unterteilt. Das primäre Fenster (rechts) zeigt Informationen zu den im Hauptmenü (links) ausgewählten Optionen an.

Im Folgenden werden die Optionen des Hauptmenüs beschrieben:

- **Startseite** - liefert Informationen zum Schutzstatus Ihres Computers, der Firewall, zum Web- und E-Mail-Schutz sowie zur Kindersicherung
- **Computer prüfen** - In diesem Bereich können Sie bei Bedarf eine On-Demand-Prüfung 8 starten oder die Einstellungen dazu ändern.
- **Update** - Informationen über Updates der Signaturdatenbank.
- **Einstellungen** - Wählen Sie diese Option, um die Sicherheitsstufe Ihres Computers anzupassen.
- **Tools** - Zugriff auf Log-Dateien 17, Taskplaner 18, Quarantäne 19, Ausgeführte Prozesse 19 und andere Programmfunktionen.
- **Hilfe** - Zugriff auf die Hilfedateien, die Internet-Knowledgebase, Supportanfrageformulare und zusätzliche Informationen zum Programm.

## 5.1 Tastaturbefehle

Folgende Tastaturbefehle können in Verbindung mit ESET Cyber Security Pro verwendet werden:

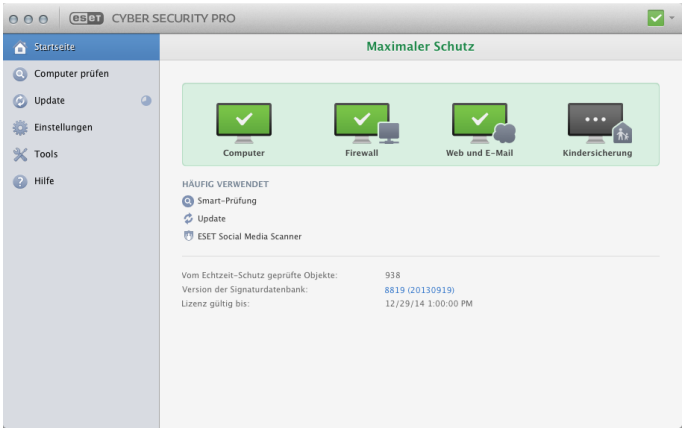
- *cmd+,* - ESET Cyber Security Pro-Einstellungen anzeigen
- *cmd+U* - öffnet das Fenster **Lizenzdaten eingeben**
- *cmd+alt+T* - öffnet das Fenster **Sonderzeichen**
- *cmd+O* - setzt das Hauptprogrammfenster von ESET Cyber Security Pro auf die Standardgröße zurück und positioniert es in der Bildschirmmitte
- *cmd+alt+H* - blendet alle offenen Fenster außer ESET Cyber Security Pro aus
- *cmd+H* - blendet ESET Cyber Security Pro aus

Die folgenden Tastaturbefehle arbeiten nur, wenn die Option **Standardmenü verwenden** unter **Einstellungen** > **Erweiterte Einstellungen ...** (oder *cmd+,* drücken) > **Schnittstelle** aktiviert ist:

- *cmd+alt+L* - öffnet das Fenster **Log-Dateien**
- *cmd+alt+S* - öffnet das Fenster **Taskplaner**
- *cmd+alt+Q* - öffnet das Fenster **Quarantäne**

## 5.2 Schutzstatus prüfen

Zum Anzeigen des Schutzstatus klicken Sie auf die Option **Startseite** im Hauptmenü. Im primären Fenster wird eine Darstellung des aktuellen Betriebszustands von ESET Cyber Security Pro angezeigt.




## 5.3 Vorgehensweise bei fehlerhafter Ausführung des Programms

Wenn die aktivierten Module ordnungsgemäß arbeiten, sind sie mit einem grün hinterlegten Häkchen markiert. Andernfalls wird ein rotes Ausrufezeichen oder orangefarbenes Warnsymbol angezeigt. Zusätzlich werden in diesem Fall weitere Informationen zu dem Modul und ein Lösungsvorschlag angezeigt. Um den Status einzelner Module zu ändern, klicken Sie auf den blauen Link unter dem jeweiligen Hinweis.

Wenn Sie ein Problem mit den vorgeschlagenen Lösungen nicht beseitigen können, können Sie in der ESET-Knowledgebase danach suchen oder sich an den ESET-Support wenden. Der Support widmet sich umgehend Ihrem Anliegen, um schnell eine Lösung für Ihr Problem zu finden.

# 6. Computerschutz

Die Computerkonfiguration finden Sie unter **Einstellungen** > **Computer**. Dort wird der Status für die Optionen **Echtzeit-Dateischutz** und **Sperren von Wechselmedien** angezeigt. Um die einzelnen Module zu deaktivieren, ändern Sie den Status des gewünschten Moduls in **DEAKTIVIERT**. Beachten Sie bitte, dass der optimale Schutz Ihres Computers dadurch möglicherweise nicht mehr gewährleistet ist. Um auf die einzelnen Einstellungen für jedes Modul zuzugreifen, klicken Sie auf **Einstellungen**.

## 6.1 Viren- und Spyware-Schutz

Der Virenschutz bewahrt das System vor Attacken, indem er potenziell gefährliche Dateien verändert. Wird eine Bedrohung durch Schadcode erkannt, kann das Virenschutz-Modul den Code unschädlich machen, indem es die Ausführung des Codes blockiert und dann den Code entfernt bzw. die Datei löscht oder in die Quarantäne verschiebt.

### 6.1.1 Allgemein

Im Bereich **Allgemein** (**Einstellungen** > **Erweiterte Einstellungen...** > **Allgemein**) können Sie die Erkennung der folgenden Arten von Anwendungen aktivieren:

- **Eventuell unerwünschte Anwendungen** - Diese Anwendungen sind nicht unbedingt und absichtlich schädlich, können jedoch die Leistung Ihres Computers negativ beeinflussen. Als Benutzer werden Sie normalerweise vor deren Installation zur Bestätigung aufgefordert. Nach erfolgter Installation ändert sich das Systemverhalten (im Vergleich zum Verhalten vor der Installation). Dazu zählen vor allem ungewollte Popup-Fenster, die Aktivierung und Ausführung versteckter Prozesse, die erhöhte Inanspruchnahme von Systemressourcen, Änderungen in Suchergebnissen sowie die Kommunikation von Anwendungen mit Remote-Servern.
- **Potenziell unsichere Anwendungen** - In diese Kategorie fallen legitime Programme seriöser Hersteller, die jedoch von Angreifern ausgenutzt werden können, wenn sie ohne Wissen des Benutzers installiert werden. Da hierzu auch Programme für die Fernsteuerung von Computern gehören, ist diese Option standardmäßig deaktiviert.
- **Verdächtige Anwendungen** - Hierunter fallen Anwendungen, die mit sogenannten "Packer"- oder "Protector"-Programmen komprimiert wurden. Diese Art von Programmen wird oft von Malware-Autoren ausgenützt, um einer Erkennung zu entgehen. Packer sind selbst-extrahierende Anwendungen, die zur Laufzeit mehrere Arten von Malware in ein einziges Paket verpacken. Die gängigsten Packer sind UPX, PE_Compact, PKLite und ASPack. Dieselbe Malware kann unter Umständen unterschiedlich erkannt werden, wenn für die Kompression ein anderer Packer verwendet wurde. Packer können außerdem die "Signaturen" regelmäßig verändern, wodurch Malware schwieriger zu erkennen und zu entfernen ist.

Klicken Sie auf **Einstellungen**, um Ausschlussfilter für Dateisystem bzw. Web- und E-Mail 7 einzurichten.

#### 6.1.1.1 Ausschlussfilter

Im Bereich **Ausschlussfilter** können Sie festlegen, dass bestimmte Dateien/Ordner, Anwendungen oder IP/IPv6-Adressen von Prüfungen ausgenommen werden.

Dateien und Ordner, die auf der Registerkarte **Dateisystem** aufgeführt sind, werden von allen Prüfungen ausgeschlossen: Prüfung der Systemstartdateien, Echtzeit-Prüfung und On-Demand-Prüfung.

- **Pfad** - Pfad zu den auszuschließenden Dateien/Ordnern
- **Bedrohung** - Steht neben einer ausgeschlossenen Datei der Name einer Bedrohung, so gilt die Ausnahme nicht generell für die Datei, sondern nur für diese bestimmte Bedrohung. Wird die Datei später durch andere Schadsoftware infiziert, erkennt der Virenschutz dies.
- **Hinzufügen...** - Objekte von der Prüfung ausnehmen. Geben Sie den Pfad zum Objekt ein (Platzhalter * und ? werden unterstützt) oder wählen Sie den Ordner bzw. die Datei in der Baumstruktur aus.
- **Bearbeiten...** - Ausgewählten Eintrag bearbeiten
- **Löschen** - Ausgewählten Eintrag löschen
- **Standard** - Alle Ausnahmen löschen

Auf der Registerkarte **Web und E-Mail** können Sie bestimmte **Anwendungen** oder **IP/IPv6-Adressen** von der Protokollprüfung ausschließen.

### 6.1.2 Systemstart-Schutz

Bei der Prüfung der Systemstartdateien werden Dateien beim Systemstart automatisch untersucht. Diese Prüfung läuft standardmäßig als geplanter Task nach der Anmeldung eines Benutzers oder nach Aktualisierungen der Viren-Datenbank. Klicken Sie auf **Einstellungen**, um die Einstellungen der ThreatSense-Engine für die Prüfung beim Systemstart zu ändern. Weitere Informationen zur Einrichtung der ThreatSense-Engine finden Sie in diesem Abschnitt 10.

### 6.1.3 Echtzeit-Dateischutz

Der Echtzeit-Dateischutz überwacht alle Datenträger auf das Eintreten bestimmter Ereignisse. Durch die Verwendung unterschiedlicher ThreatSense-Technologien (siehe Abschnitt ThreatSense-Einstellungen 10) kann der Echtzeit-Dateischutz für neu erstellte Dateien von dem für bestehende Dateien abweichen. Neu erstellte Dateien können einer noch gründlicheren Prüfung unterzogen werden.

Der Echtzeit-Dateischutz wird standardmäßig beim Systemstart gestartet und fortlaufend ausgeführt. In besonderen Fällen (z. B. bei einem Konflikt mit einem anderen Echtzeit-Prüfprogramm) kann der Echtzeit-Dateischutz durch Klicken auf das ESET Cyber Security Pro-Symbol in der oberen Menüleiste und Auswählen der Option **Echtzeit-Dateischutz deaktivieren** beendet werden. Der Echtzeit-Dateischutz lässt sich auch im Hauptfenster beenden. Klicken Sie dazu auf **Einstellungen** > **Computer** und setzen Sie die Option **Echtzeit-Dateischutz** auf **DEAKTIVIERT**.

Um die erweiterten Einstellungen für den Echtzeit-Dateischutz zu ändern, wechseln Sie zu **Einstellungen** > **Erweiterte Einstellungen ...** (oder drücken *cmd+,*) > **Echtzeit-Schutz** und klicken neben **Erweiterte Einstellungen ...** auf **Einstellungen** (siehe Abschnitt Erweiterte Einstellungen für Prüfungen 8).

#### 6.1.3.1 Prüfen beim (Prüfen bei Ereignis)

Standardmäßig werden alle Dateien beim Öffnen, Erstellen und Ausführen geprüft. Wir empfehlen Ihnen, die Standardeinstellungen beizubehalten. So bietet der Echtzeit-Dateischutz auf Ihrem Computer maximale Sicherheit.

#### 6.1.3.2 Erweiterte Einstellungen

In diesem Fenster können Sie die vom ThreatSense-Prüfmodul zu prüfenden Objekttypen festlegen, die **Advanced Heuristik** aktivieren bzw. deaktivieren sowie die Einstellungen für Archive und den Datei-Cache ändern.

Die Standardwerte im Abschnitt **Standard-Archiveinstellungen** sollten Sie nur ändern, um konkrete Probleme zu lösen, da höhere Archivverschachtelungswerte die Systemleistung beeinträchtigen können.

Sie können die ThreatSense Advanced Heuristik für ausführbare, erstellte und geänderte Dateien einzeln ein- bzw. ausschalten. Aktivieren Sie dazu jeweils das Kontrollkästchen **Advanced Heuristik** im Abschnitt der entsprechenden ThreatSense-Einstellungen.

Um eine möglichst geringe Systembelastung während des Echtzeit-Dateischutzes zu gewährleisten, können Sie die Größe des Optimierungs-Cache festlegen. Dieses Verhalten ist aktiv, wenn Sie die Option **Cache für nicht infizierte Dateien aktivieren** verwenden. Ist diese Option deaktiviert, werden alle Dateien bei jedem Zugriff geprüft. Ansonsten werden nicht infizierte Dateien bis zur festgelegten Cache-Größe im Cache gespeichert und anschließend nicht mehr geprüft, es sei denn, sie wurden geändert. Nach einem Update der Signaturdatenbank werden die Dateien sofort wieder geprüft. Klicken Sie auf **Cache für nicht infizierte Dateien aktivieren**, um diese Funktion zu aktivieren bzw. deaktivieren. Um die Anzahl der Dateien festzusetzen, die im Cache gespeichert werden sollen, geben Sie einfach den gewünschten Wert ins Feld **Cache-Größe** ein.

Zusätzliche Prüfparameter können im Fenster **ThreatSense-Einstellungen** festgelegt werden. Sie können angeben, welche Typen von **Objekten** geprüft werden sollen, mit welchen **Optionen** und auf welcher **Säuberungsstufe**. Außerdem können Sie die **Erweiterungen** und **Grenzen** für Dateigrößen für den Echtzeit-Dateischutz definieren. Das Fenster mit den ThreatSense-Einstellungen erreichen Sie über die Schaltfläche **Einstellungen** neben **ThreatSense-Prüfmodul** im Fenster **Erweiterte Einstellungen**. Ausführliche Informationen zu den ThreatSense-Einstellungen finden Sie im Abschnitt ThreatSense-Einstellungen 10.

#### 6.1.3.3 Wann sollten die Einstellungen für den Echtzeit-Dateischutz geändert werden?

Der Echtzeit-Dateischutz ist die wichtigste Komponente für ein sicheres System. Änderungen an den Parametern des Echtzeit-Dateischutzes sind mit Bedacht vorzunehmen. Es wird empfohlen, nur in einzelnen Fällen die Parameter zu verändern. Es kann beispielsweise erforderlich sein, wenn ein Konflikt mit einer bestimmten Anwendung oder der Echtzeit-Prüfung eines anderen Virenschutzprogramms vorliegt.

Bei der Installation von ESET Cyber Security Pro werden alle Einstellungen optimal eingerichtet, um dem Benutzer die größtmögliche Schutzstufe für das System zu bieten. Um die Standardeinstellungen wiederherzustellen, klicken Sie auf die Schaltfläche **Standard** unten links im Fenster **Echtzeit-Dateischutz** (**Einstellungen** > **Erweiterte Einstellungen** > **Echtzeit-Schutz**).

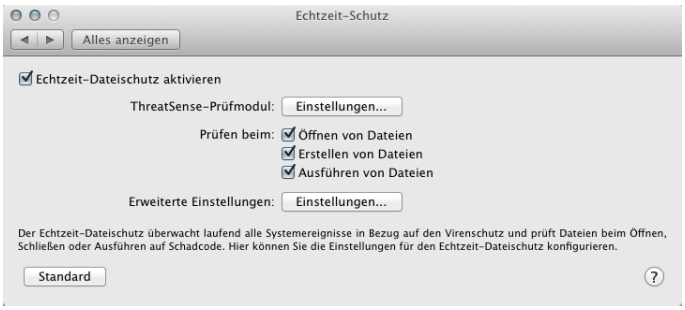
#### 6.1.3.4 Echtzeit-Dateischutz prüfen

Um sicherzustellen, dass der Echtzeit-Dateischutz aktiv ist und Viren erkennt, verwenden Sie die Testdatei eicar.com. Diese Testdatei ist harmlos und wird von allen Virenschutzprogrammen erkannt. Die Datei wurde vom EICAR-Institut (European Institute for Computer Antivirus Research) erstellt, um die Funktionalität von Virenschutzprogrammen zu testen.

#### 6.1.3.5 Vorgehensweise bei fehlerhaftem Echtzeit-Dateischutz

In diesem Kapitel werden mögliche Probleme mit dem Echtzeit-Dateischutz sowie Lösungsstrategien beschrieben.

**Echtzeit-Dateischutz ist deaktiviert**
Der Echtzeit-Dateischutz wurde versehentlich von einem Benutzer deaktiviert und muss reaktiviert werden. Um den Echtzeit-Schutz erneut zu aktivieren, setzen Sie die Option **Echtzeit-Dateischutz** (unter **Einstellungen** > **Computer**) auf **AKTIVIERT**. Alternativ dazu können Sie den Echtzeit-Dateischutz im Fenster **Erweiterte Einstellungen** unter **Echtzeit-Schutz** aktivieren. Wählen Sie dazu die Option **Echtzeit-Dateischutz aktivieren**.


Echtzeit-Schutz
Alles anzeigen
Echtzeit-Dateischutz aktivieren
ThreatSense-Prüfmodul:
Einstellungen...
Prüfen beim:
Öffnen von Dateien
Erstellen von Dateien
Ausführen von Dateien
Erweiterte Einstellungen:
Einstellungen...
Der Echtzeit-Dateischutz überwacht laufend alle Systemereignisse in Bezug auf den Virenschutz und prüft Dateien beim Öffnen, Schließen oder Ausführen auf Schadcode. Hier können Sie die Einstellungen für den Echtzeit-Dateischutz konfigurieren.
Standard

**Echtzeit-Dateischutz erkennt und entfernt keinen Schadcode**
Stellen Sie sicher, dass keine anderen Virenschutzprogramme auf Ihrem Computer installiert sind. Zwei parallel ausgeführte Schutzprogramme können miteinander in Konflikt geraten. Wir empfehlen Ihnen, alle anderen Virusschutzprogramme zu deinstallieren.

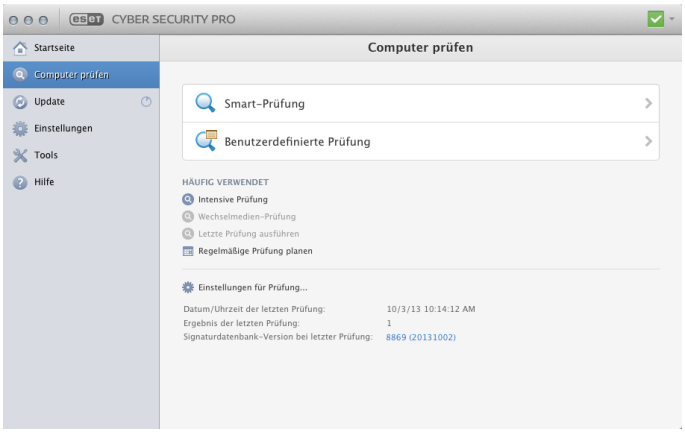
**Echtzeit-Dateischutz startet nicht**
Wenn der Echtzeit-Dateischutz nicht automatisch beim Systemstart startet, können Konflikte mit anderen Programmen vorliegen. Sollte dies der Fall sein, wenden Sie sich an einen der Experten vom ESET-Support.

### 6.1.4 On-Demand-Prüfung

Wenn Sie den Verdacht haben, dass Ihr Computer infiziert ist (anormales Verhalten), starten Sie über **Computer prüfen** > **Smart-Prüfung** eine manuelle Prüfung, um Ihren Computer auf eingedrungene Schadsoftware zu untersuchen. Um maximalen Schutz zu gewährleisten, sollten Sie solche Prüfungen routinemäßig durchführen und nicht nur, wenn eine Infektion vermutet wird. Durch regelmäßige Prüfungen kann eingedrungene Schadsoftware erkannt werden, die vom Echtzeit-Dateischutz zum Zeitpunkt der Speicherung der

Schadsoftware nicht erkannt wurde. Dies kommt z. B. vor, wenn die Echtzeit-Prüfung zum Zeitpunkt der Infektion deaktiviert war oder die Signaturdatenbank nicht auf dem neuesten Stand ist.

Sie sollten mindestens einmal im Monat eine On-Demand-Prüfung vornehmen. Sie können die Prüfung als Task unter **Tools** > **Taskplaner** konfigurieren.




Sie können auch ausgewählte Dateien und Ordner von Ihrem Desktop oder aus dem **Finder**-Fenster per Drag & Drop auf dem Hauptbildschirm, Dock-Symbol, Menüleistensymbol (oberer Bildschirmrand) oder Anwendungssymbol (im Ordner */Anwendungen*) von ESET Cyber Security Pro ablegen.

### 6.1.4.1 Prüfungstyp

Es gibt zwei verschiedene Arten von On-Demand-Prüfungen. Bei der **Smart-Prüfung** (Standardprüfung) wird das System schnell überprüft, ohne dass Sie dafür weitere Prüfparameter konfigurieren müssen. Bei der Methode **Prüfen mit speziellen Einstellungen** können Sie ein vordefiniertes Prüfprofil und die zu prüfenden Objekte auswählen.

#### 6.1.4.1.1 Smart-Prüfung

Mit der Smart-Prüfung (Standardprüfung) können Sie schnell den Computer prüfen und infizierte Dateien säubern, ohne eingreifen zu müssen. Die Bedienung ist einfach, und es ist keine ausführliche Konfiguration erforderlich. Bei der Smart-Prüfung werden alle Dateien in allen Ordnern geprüft, und erkannte Infiltrationen werden automatisch entfernt. Als Säuberungsstufe wird automatisch der Standardwert festgelegt. Weitere Informationen zu den Säuberungsarten finden Sie unter Säubern 10.

#### 6.1.4.1.2 Prüfen mit speziellen Einstellungen

Über die Option **Prüfen mit speziellen Einstellungen** können Sie Prüfparameter wie die zu prüfenden Objekte oder Prüfmethoden festlegen. Der Vorteil dieser Methode ist die Möglichkeit zur genauen Parameterkonfiguration. Verschiedene Konfigurationen können als benutzerdefinierte Prüfprofile gespeichert werden. Das ist sinnvoll, wenn Prüfungen wiederholt mit denselben Parametern ausgeführt werden.

Zum Festlegen der zu prüfenden Objekte wählen Sie **Computer prüfen** > **Prüfen mit speziellen Einstellungen** und wählen dann bestimmte **Zu prüfende Objekte** aus der Baumstruktur aus. Sie können ein zu prüfendes Objekt auch genauer bestimmen, indem Sie den Pfad zu dem Ordner oder den Dateien eingeben, die geprüft werden sollen. Wenn Sie nur das System ohne zusätzliche Säuberung prüfen möchten, wählen Sie die Option **Nur Prüfen, keine Aktion**. Außerdem können Sie zwischen drei Säuberungsstufen wählen. Klicken Sie dazu auf **Einstellungen** > **Säubern**.

**HINWEIS:** Eine Prüfung des Computers mit dieser Methode wird nur fortgeschrittenen Benutzern empfohlen, die Erfahrung im Umgang mit Virenschutzprogrammen haben.

### 6.1.4.2 Zu prüfende Objekte

In der Baumstruktur der zu prüfenden Objekte können Sie Dateien und Ordner auswählen, die auf Viren geprüft werden sollen. Im Prüfprofil können Sie die Prüfung von Ordnern festlegen.

Sie können ein zu prüfendes Objekt auch genauer definieren, indem Sie den Pfad zu dem Ordner oder den Dateien eingeben, die geprüft werden sollen. Wählen Sie die zu prüfenden Objekte aus der Baumstruktur aus, in der alle auf dem Computer verfügbaren Ordner aufgelistet werden.

### 6.1.4.3 Prüfprofile

Ihre benutzerdefinierten Einstellungen können für zukünftige Prüfungen gespeichert werden. Wir empfehlen Ihnen, für jede regelmäßig durchgeführte Prüfung ein eigenes Profil zu erstellen (mit verschiedenen zu prüfenden Objekten, Prüfmethoden und anderen Parametern).

Zur Erstellung eines neuen Profils klicken Sie im Hauptmenü auf **Einstellungen** > **Erweiterte Einstellungen ...** (oder drücken *cmd+,*) > **Computer prüfen** und klicken auf **Bearbeiten...** neben der Liste der aktuell bestehenden Profile.

Computer prüfen
Alles anzeigen
Profil für Smart-Prüfung:
Smart-Prüfung
Bearbeiten...
Einstellungen für Prüfprofile
Prüfprofil:
Smart-Prüfung
ThreatSense-Prüfmodul: Einstellungen...
Zu prüfende Objekte: Einstellungen...
Die On-Demand-Prüfung dient zur Prüfung von Dateien und Ordnern auf dem Computer. Zum Starten verwenden Sie den Befehl 'Computer prüfen' im Hauptfenster. Hier können Sie die Einstellungen für die On-Demand-Prüfung konfigurieren.
Standard

Eine Beschreibung der einzelnen Prüfeinstellungen finden Sie im Abschnitt ThreatSense-Einstellungen 10. So können Sie ein Prüfprofil erstellen, das auf Ihre Anforderungen zugeschnitten ist.

Beispiel: Nehmen wir an, Sie möchten Ihr eigenes Prüfprofil erstellen. Die Smart-Prüfung eignet sich in gewissem Maße, aber Sie möchten nicht die laufzeitkomprimierten Dateien oder potenziell unsichere Anwendungen prüfen. Außerdem möchten Sie die Option „Automatisch säubern“ anwenden. Geben Sie im Fenster **Profile für On-Demand-Scanner** den Profilnamen ein, klicken Sie auf **Hinzufügen** und bestätigen Sie mit **OK**. Passen Sie dann die Parameter unter **ThreatSense-Prüfmodul** und **Zu prüfende Objekte** an Ihre Anforderungen an.

### 6.1.5 ThreatSense-Einstellungen

ThreatSense ist eine proprietäre Technologie von ESET und besteht aus einer Kombination hochentwickelter Bedrohungserkennungsmethoden. Diese Prüftechnologie arbeitet proaktiv, d. h., sie schützt das System auch während der ersten Stunden eines neuen Angriffs. Eingesetzt wird eine Kombination verschiedener Methoden (Code-Analyse, Code-Emulation, allgemeine Signaturen, Virussignaturen), die zusammen die Systemsicherheit deutlich erhöhen. Das Prüfmodul kann verschiedene Datenströme gleichzeitig kontrollieren und so die Effizienz und Erkennungsrate steigern. Die ThreatSense-Technologie entfernt auch Rootkits erfolgreich.

In den ThreatSense-Einstellungen können Sie verschiedene Prüfparameter festlegen:

- Dateitypen und -erweiterungen, die geprüft werden sollen
- Die Kombination verschiedener Erkennungsmethoden
- Säuberungsstufen usw.

Zum Öffnen der Einstellungen klicken Sie auf **Einstellungen > Erweiterte Einstellungen ...** (oder drücken *cmd+,*) und klicken anschließend auf die Schaltfläche **Einstellungen** für das ThreatSense-Prüfmodul im Bereich **Systemstart-Schutz**, **Echtzeit-Schutz** bzw. **Computer prüfen**, die alle die ThreatSense-Technologie verwenden (siehe unten). Je nach Anforderung sind eventuell verschiedene Sicherheitseinstellungen erforderlich. Dies sollte bei den individuellen ThreatSense-Einstellungen für die folgenden Schutzmodule berücksichtigt werden:

- **Systemstart-Schutz** - Automatische Prüfung der Systemstartdateien
- **Echtzeit-Schutz** - Echtzeit-Dateischutz
- **Computer prüfen** - On-Demand-Prüfung

Die ThreatSense-Einstellungen sind für jedes Modul optimal eingerichtet, und eine Veränderung der Einstellungen kann den Systembetrieb deutlich beeinflussen. So kann zum Beispiel eine Änderung der Einstellungen für das Prüfen laufzeitkomprimierter Dateien oder die Aktivierung der Advanced Heuristik im Echtzeit-Dateischutz dazu führen, dass das System langsamer arbeitet. Es wird daher empfohlen, die ThreatSense-Standardeinstellungen für alle Module unverändert beizubehalten. Änderungen sollten nur im Modul „Computer prüfen“ vorgenommen werden.

#### 6.1.5.1 Objekte

Im Bereich **Objekte** können Sie festlegen, welche Dateien auf Infiltrationen geprüft werden sollen.

- **Dateien** - Prüfung der gängigen Dateitypen (Programm-, Bild-, Audio-, Video-, Datenbankdateien usw.).
- **Symbolische Links** - (Nur bei On-Demand-Prüfung) Prüfung spezieller Dateitypen, die eine Textfolge enthalten, die vom Betriebssystem ausgewertet und als Pfad zu einer anderen Datei oder einem anderen Verzeichnis genutzt wird.
- **E-Mail-Dateien** - (nicht verfügbar in Echtzeit-Dateischutz) Prüfung von Dateien, die E-Mail-Nachrichten enthalten.
- **Postfächer** - (nicht verfügbar in Echtzeit-Dateischutz) Prüfung von Benutzerpostfächern im System. Die unsachgemäße Anwendung dieser Option kann zu Konflikten mit Ihrem E-Mail-Programm führen. Für weitere Informationen über Vor- und Nachteile dieser Option lesen Sie den folgenden Knowledgebase-Artikel.
- **Archive** - (nicht verfügbar in Echtzeit-Dateischutz) Prüfung von komprimierten Archivdateien (.rar, .zip, .arj, .tar usw.).
- **Selbstentpackende Archive** - (nicht verfügbar in Echtzeit-Dateischutz) Prüfung von Dateien in selbstentpackenden Archiven.
- **Laufzeitkomprimierte Dateien** - Laufzeitkomprimierte Dateien werden (anders als Standard-Archivtypen) im Arbeitsspeicher dekomprimiert, zusätzlich zu statisch laufzeitkomprimierten Dateien (UPX, yoda, ASPack, FGS etc.).

#### 6.1.5.2 Optionen

Im Bereich **Optionen** können Sie die Methoden festlegen, die bei einer Prüfung des Systems auf Infiltrationen angewendet werden sollen. Die folgenden Optionen stehen zur Verfügung:

- **Heuristik** - Heuristische Methoden verwenden einen Algorithmus, der (bösartige) Aktivitäten von Programmen analysiert. Mit ihrer Hilfe können bis dato unbekannte Schadprogramme oder Viren, die nicht in der Liste bekannter Viren (Signaturdatenbank) aufgeführt waren, erkannt werden.
- **Advanced Heuristik** - Als Advanced Heuristik werden besondere, von ESET entwickelte heuristische Verfahren bezeichnet, die für die Erkennung von Würmern und Trojanern optimiert sind, die in höheren Programmiersprachen geschrieben wurden. Die Erkennungsrate des Programms ist dadurch wesentlich gestiegen.
- **ESET Live Grid** - Durch das Live Grid-Frühwarnsystem ist ESET beim Auftauchen neuer Infiltrationen immer auf dem neuesten Stand und kann seine Kunden schneller schützen. Weitere Informationen finden Sie im Bereich Live Grid 20.

#### 6.1.5.3 Säubern

In den Säuberungseinstellungen wird festgelegt, wie der Scanner die infizierten Dateien säubert. Es gibt drei Arten der Schadcodeentfernung:

- **Nicht säubern** - Der in infizierten Objekten erkannte Schadcode wird nicht automatisch entfernt. Eine Warnung wird angezeigt, und Sie werden aufgefordert, eine Aktion auszuwählen.

- **Normales säubern** - Das Programm versucht, den Schadcode automatisch aus der Datei zu entfernen oder eine infizierte Datei zu löschen. Wenn es nicht möglich ist, die passende Aktion automatisch zu bestimmen, wird der Benutzer aufgefordert, eine Aktion auszuwählen. Diese Auswahl wird dem Benutzer auch dann angezeigt, wenn eine vordefinierte Aktion nicht erfolgreich abgeschlossen werden konnte.
- **Automatisch säubern** - Das Programm entfernt den Schadcode aus infizierten Dateien oder löscht diese Dateien (einschließlich Archiven). Ausnahmen gelten nur für Systemdateien. Wenn es nicht möglich ist, den Schadcode zu entfernen, werden Sie in der angezeigten Warnung aufgefordert, eine Aktion auszuwählen.

***Warnung:*** Im Standardmodus „Normales Säubern" wird das gesamte Archiv nur gelöscht, wenn es ausschließlich infizierte Dateien enthält. Sind auch nicht infizierte Dateien vorhanden, wird die Archivdatei nicht gelöscht. Im Modus „Automatisch säubern" wird die gesamte Archivdatei gelöscht, auch wenn sie nicht infizierte Dateien enthält.

#### 6.1.5.4 Erweiterungen

Die Erweiterung ist der Teil eines Dateinamens nach dem Punkt. Die Erweiterung definiert Typ und Inhalt der Datei. In diesem Teil der ThreatSense-Einstellungen können Sie die Dateitypen festlegen, die nicht geprüft werden sollen.

In der Standardeinstellung werden alle Dateien unabhängig von ihrer Erweiterung geprüft. Jede Erweiterung kann der Liste auszuschließender Dateien hinzugefügt werden. Über die Schaltflächen **Hinzufügen** und **Entfernen** können Sie festlegen, welche Erweiterungen geprüft werden sollen.

Der Ausschluss bestimmter Dateien ist dann sinnvoll, wenn die Prüfung bestimmter Dateitypen die Funktion eines Programms beeinträchtigt. Es macht zum Beispiel Sinn, die Erweiterungen *.log*, *.cfg* und *.tmp* auszuschließen. Das korrekte Format für die Angabe von Dateierweiterungen ist: **.log*, **.cfg*, **.tmp*.

#### 6.1.5.5 Grenzen

Im Bereich **Grenzen** können Sie die Maximalgröße von Elementen und Stufen verschachtelter Archive festlegen, die geprüft werden sollen:

- **Maximale Größe:** Definiert die maximale Größe von zu prüfenden Objekten. Der Virenschutz prüft dann nur die Elemente, deren Größe unter der angegebenen Maximalgröße liegt. Der Standardwert sollte nicht geändert werden; für gewöhnlich besteht dazu auch kein Grund. Diese Option sollte nur von fortgeschrittenen Benutzern geändert werden, die bestimmte Gründe dafür haben, größere Objekte von der Prüfung auszuschließen.
- **Maximale Prüfzeit:** Definiert die maximale Dauer, die für die Prüfung eines Objekts zur Verfügung steht. Wenn hier ein benutzerdefinierter Wert eingegeben wurde, beendet der Virenschutz die Prüfung eines Elements, sobald diese Zeit abgelaufen ist, und zwar ungeachtet dessen, ob die Prüfung abgeschlossen ist oder nicht.
- **Maximale Verschachtelungstiefe:** Legt die maximale Tiefe der Archivprüfung fest. Der Standardwert 10 sollte nicht geändert werden; unter normalen Umständen besteht dazu auch kein Grund. Wenn die Prüfung aufgrund der Anzahl verschachtelter Archive vorzeitig beendet wird, bleibt das Archiv ungeprüft.
- **Maximale Dateigröße:** Über diese Option können Sie die maximale Dateigröße der entpackten Dateien festlegen, die in zu prüfenden Archiven enthalten sind. Wenn die Prüfung aufgrund dieses Grenzwerts vorzeitig beendet wird, bleibt das Archiv ungeprüft.

#### 6.1.5.6 Sonstige

**Smart-Optimierung aktivieren**
Die Smart-Optimierung passt die Einstellungen so an, dass eine wirksame Prüfung bei gleichzeitig hoher Prüfgeschwindigkeit gewährleistet ist. Die verschiedenen Schutzmodule prüfen auf intelligente Weise unter Einsatz verschiedener Prüfmethoden. Die Smart-Optimierung ist innerhalb des Produkts nicht starr definiert. Das ESET-Entwicklungsteam fügt ständig neue Ergänzungen hinzu, die dann über die regelmäßigen Updates in ESET Cyber Security Pro integriert werden. Wenn die Smart-Optimierung deaktiviert ist, werden nur die benutzerdefinierten Einstellungen im ThreatSense-Kern des entsprechenden Moduls für die Prüfung verwendet.

**Alternative Datenströme (ADS) prüfen** (Nur bei On-Demand-Prüfung)
Bei den von Dateisystemen verwendeten alternativen Datenströmen (Ressourcen-/Daten-Forks) handelt es sich um Datei- und Ordnerzuordnungen, die mit herkömmlichen Prüftechniken nicht erkannt werden können. Eingedrungene Schadsoftware tarnt sich häufig als alternativer Datenstrom, um nicht erkannt zu werden.

### 6.1.6 Eingedrungene Schadsoftware wurde erkannt

Schadsoftware kann auf vielen Wegen in das System gelangen. Mögliche Infektionswege sind Webseiten, freigegebene Ordner, E-Mails oder Wechselmedien (USB-Sticks, externe Festplatten, CDs, DVDs usw.).

Wenn Ihr Computer die Symptome einer Malware-Infektion aufweist (Computer arbeitet langsamer als gewöhnlich, hängt sich oft auf usw.), sollten Sie folgendermaßen vorgehen:

1. Klicken Sie auf **Computer prüfen**.
2. Klicken Sie auf **Smart-Prüfung** (weitere Informationen siehe Abschnitt Smart-Prüfung 9).
3. Nachdem die Prüfung abgeschlossen ist, überprüfen Sie im Log die Anzahl der geprüften, infizierten und gesäuberten Dateien.

Wenn Sie nur einen Teil Ihrer Festplatte prüfen möchten, wählen Sie **Prüfen mit speziellen Einstellungen** und anschließend die Bereiche, die auf Viren geprüft werden sollen.

Das folgende allgemeine Beispiel soll veranschaulichen, wie in ESET Cyber Security Pro mit Schadsoftware umgegangen wird. Nehmen wir einmal an, der Echtzeit-Dateischutz verwendet die Standard-Säuberungsstufe und erkennt eingedrungene Schadsoftware. Daraufhin wird der Versuch gestartet, den Schadcode aus der Datei zu entfernen oder die Datei zu löschen. Ist für den Echtzeitschutz keine vordefinierte

Aktion angegeben, müssen Sie in einem Warnungsfenster zwischen verschiedenen Optionen wählen. In der Regel stehen die Optionen **Säubern**, **Löschen** und **Keine Aktion** zur Auswahl. Es wird nicht empfohlen, die Option **Keine Aktion** zu wählen, da sonst die infizierten Dateien nicht behandelt werden. Einzige Ausnahme: Sie sind sich sicher, dass die Datei harmlos ist und versehentlich erkannt wurde.

**Säubern und löschen** - Wählen Sie „Säubern“, wenn eine Datei von einem Virus mit Schadcode infiziert wurde. In einem solchen Fall sollten Sie zuerst versuchen, den Schadcode aus der infizierten Datei zu entfernen und ihren Originalzustand wiederherzustellen. Wenn die Datei ausschließlich Schadcode enthält, wird sie gelöscht.

**Dateien in Archiven löschen** - Im Standardmodus der Aktion „Säubern“ wird das gesamte Archiv nur gelöscht, wenn es ausschließlich infizierte Dateien enthält. Archive, die auch nicht infizierte Dateien enthalten, werden also nicht gelöscht. Die Option **Automatisch säubern** sollten Sie hingegen mit Bedacht einsetzen, da in diesem Modus alle Archive gelöscht werden, die mindestens eine infizierte Datei enthalten, und zwar unabhängig vom Status der übrigen Archivdateien.

### 6.2 Prüfen und Sperren von Wechselmedien

ESET Cyber Security Pro unterstützt eine On-Demand-Prüfung von angeschlossenen Wechselmedien (CD, DVD, USB, iOS-Geräte usw.).

Auf Wechselmedien kann sich Schadcode befinden, der eine Gefahr für Ihren Computer darstellt. Um Wechselmedien zu sperren, klicken Sie im Hauptfenster auf **Einstellungen für Wechselmedien-Sperre** (siehe Abbildung oben) oder **Einstellungen** > **Erweiterte Einstellungen** > **Medien** und aktivieren Sie die Option **Sperre für Wechselmedien aktivieren**. Um den Zugriff auf bestimmte Medientypen zuzuzulassen, deaktivieren Sie das dazugehörige Kontrollkästchen.

**HINWEIS:** Wenn Sie den Zugriff auf externe CD-ROM-Laufwerke, die über ein USB-Kabel an Ihren Computer angeschlossen sind, zulassen möchten, deaktivieren Sie die Option **CD-ROM**.

## 7. Phishing-Schutz

Der Ausdruck *Phishing* bezeichnet kriminelle Vorgehensweisen unter Verwendung von Social-Engineering-Techniken (Manipulation von Anwendern, um an vertrauliche Daten zu gelangen). Phishing zielt darauf ab, an vertrauliche Daten wie Konto- und Kreditkartennummern, PIN-Codes, Benutzernamen und Passwörter usw. zu gelangen.

Wir empfehlen, den Phishing-Schutz aktiviert zu lassen ( **Einstellungen** > **Erweiterte Einstellungen ...** > **Phishing-Schutz**). Alle potenziellen Phishing-Angriffe von Webseiten oder Domänen, die in der ESET-Malwaredatenbank aufgeführt sind, werden blockiert, und Sie erhalten einen Warnhinweis über den Angriffsversuch.

## 8. Firewall

Die Personal Firewall überwacht den gesamten Datenverkehr zum und vom System. Dazu werden die einzelnen Netzwerkverbindungen gemäß festgelegten Filterregeln entweder zugelassen oder blockiert. So bietet die Firewall Schutz gegen Angriffe von Remotecomputern und ermöglicht das Blockieren bestimmter Dienste. Darüber hinaus bietet sie einen Virenschutz für die Protokolle HTTP, POP3 und IMAP. Diese Funktionen stellen ein wichtiges Element der Sicherheit eines Computers dar.

Die Konfiguration für die Personal Firewall finden Sie unter **Einstellungen** > **Firewall**. Dort können Sie den Filtermodus auswählen, Regeln festlegen und weitere Einstellungen vornehmen. Außerdem können Sie auf genauere Einstellungen des Programms zugreifen.

Wenn Sie die Option **Alle Netzwerkverbindungen blockieren: vom Netzwerk trennen** auf **AKTIVIERT** setzen, wird der gesamte ein- und ausgehende Datenverkehr von der Personal Firewall blockiert. Verwenden Sie diese Option nur bei Verdacht auf eine ernste Bedrohung, bei der das System vom Netzwerk getrennt werden muss.

### 8.1 Filtermodi

Für die ESET Cyber Security Pro-Personal Firewall stehen drei Filtermodi zur Auswahl. Sie finden die Filtermodieinstellungen in den ESET Cyber Security Pro-Einstellungen (drücken Sie *cmd+,*) > **Firewall**. Das Verhalten der Firewall ändert sich je nach gewähltem Modus. Der Filtermodus bestimmt auch, wie stark der Anwender eingreifen muss.

**Alle Verbindungen blockiert** - Sämtliche ein- und ausgehenden Verbindungen werden blockiert.

**Automatisch mit Ausnahmen** - Dies ist der Standardmodus. Dieser Modus eignet sich für Anwender, die eine möglichst einfache und praktische Nutzung der Firewall wünschen, bei der keine Regeln erstellt werden müssen. Im Automatikmodus ist der ausgehende Standarddatenverkehr für das System zugelassen und nicht initiierte Verbindungen aus dem Netzwerk werden blockiert. Sie haben auch die Möglichkeit, benutzerdefinierte Regeln hinzuzufügen.

**Interaktiv** - Mit diesem Modus können Sie eine benutzerdefinierte Konfiguration für Ihre Personal Firewall erstellen. Wenn eine Verbindung erkannt wird und keine Regel dafür existiert oder gilt, wird in einem Dialogfenster eine unbekannte Verbindung gemeldet. Das Dialogfenster enthält die Optionen, die Verbindung zuzulassen oder zu blockieren. Die getroffene Entscheidung, d. h. „zulassen“ oder „blockieren“, kann als neue Regel für die Firewall gespeichert werden. Wenn Sie zu diesem Zeitpunkt eine neue Regel erstellen möchten, werden sämtliche zukünftigen Verbindungen dieses Typs gemäß der Regel entweder zugelassen oder blockiert.

Um genaue Informationen zu allen blockierten Verbindungen in einer Log-Datei zu speichern, aktivieren Sie die Option **Alle blockierten Verbindungen in Log aufnehmen**. Um die Log-Dateien der Firewall zu prüfen, klicken Sie im Hauptmenü auf **Tools** > **Logs** und wählen Sie **Firewall** aus dem Dropdown-Menü **Log**.

## 8.2 Firewall-Regeln

Regeln definieren eine Reihe von Bedingungen, mit denen sämtliche Netzwerkverbindungen getestet werden, sowie die Aktionen im Zusammenhang mit diesen Bedingungen. Über die Personal Firewall können Sie festlegen, welche Aktion ausgeführt werden soll, wenn eine Verbindung aufgebaut wird, für die eine Regel existiert.

Eingehende Verbindungen stammen von Remotecomputern, die versuchen, eine Verbindung mit dem lokalen System aufzubauen. Ausgehende Verbindungen funktionieren umgekehrt - das lokale System nimmt Kontakt mit einem Remotecomputer auf.

Wenn eine neue unbekannte Verbindung erkannt wird, sollten Sie sich gut überlegen, ob Sie sie zulassen oder blockieren. Ungebetene, unsichere oder unbekannte Verbindungen stellen ein Sicherheitsrisiko für das System dar. Wenn eine solche Verbindung aufgebaut wurde, empfehlen wir Ihnen, genau auf den Remotecomputer und die Anwendung, die versucht, auf Ihren Computer zuzugreifen, zu achten. Viele Infiltrationen versuchen, an private Daten zu gelangen, solche Daten zu senden oder weitere Schadprogramme auf den Computer herunterzuladen. Mit der Personal Firewall können Sie solche Verbindungen erkennen und beenden.

### 8.2.1 Erstellen neuer Regeln

Die Registerkarte **Regeln** enthält eine Liste aller Regeln, die auf den Datenverkehr der einzelnen Anwendungen angewendet werden. Regeln werden automatisch gemäß der Reaktion des Anwenders bei einer neuen Verbindung hinzugefügt.

Um eine neue Regel zu erstellen, klicken Sie auf **Hinzufügen**, geben einen Namen für die Regel ein und ziehen das Symbol der Anwendung per Drag & Drop in das leere quadratische Feld. Alternativ können Sie auf **Durchsuchen** klicken, um das Programm im Verzeichnis */Programme* zu suchen. Wenn Sie die Regel auf alle Anwendungen anwenden möchten, die auf Ihrem Computer installiert sind, aktivieren Sie die Option **Alle Anwendungen**.

Wählen Sie danach die gewünschte **Aktion** (Kommunikation zwischen ausgewählter Anwendung und Netzwerk zulassen oder blockieren) und die **Richtung** des Datenverkehrs (eingehend, ausgehend oder beides). Wenn Sie alle Verbindungen im Zusammenhang mit dieser Regel in einer Log-Datei protokollieren möchten, aktivieren Sie die Option **Regel in Log schreiben**. Um die Logs zu prüfen, klicken Sie im ESET Cyber Security Pro-Hauptmenü auf **Tools** > **Logs** und wählen Sie **Firewall** aus dem Dropdown-Menü **Log**.

Wählen Sie im Bereich **Protokoll/Ports** das Protokoll aus, über das die Anwendung kommuniziert, sowie die betreffenden Portnummern (wenn TCP oder UDP ausgewählt wurde). Die Transportprotokoll-Ebene ermöglicht einen sicheren und effizienten Datentransfer.

Zum Schluss geben Sie das Ziel an (IP-Adresse/-Bereich, Subnetz, Ethernet oder Internet).

## 8.3 Firewall-Zonen

Eine Zone besteht aus einer Sammlung von Netzwerkadressen, die eine logische Gruppe ergeben. Jeder Adresse in einer Gruppe werden die gleichen Regeln zugewiesen, die zentral für die gesamte Gruppe erstellt werden.

Sie können solche Zonen erstellen, indem Sie auf die Schaltfläche **Hinzufügen** klicken. Geben Sie einen Namen im Feld **Name** und eine **Beschreibung** (optional) der Zone ein. Wählen Sie ein Profil aus, dem die Zone zugewiesen werden soll, und fügen Sie eine IPv4-/IPv6-Adresse, einen Adressbereich, ein Subnetz, ein WiFi-Netzwerk oder eine Schnittstelle hinzu.

## 8.4 Firewall-Profile

Über die Option **Profile** können Sie das Verhalten der Personal Firewall von ESET Cyber Security Pro steuern. Sie können Firewall-Regeln während der Erstellung oder Bearbeitung einem spezifischen Profil zuweisen oder für alle Profile anwenden. Wenn Sie ein Profil auswählen, werden nur die globalen Regeln (ohne ausgewähltes Profil) sowie die diesem Profil zugewiesenen Regeln angewendet. Sie können mehrere Profile mit unterschiedlichen Regeln erstellen, um das Verhalten der Personal Firewall schnell und einfach zu ändern.

## 8.5 Firewall-Logs

Die ESET Cyber Security Pro-Personal Firewall speichert alle wichtigen Ereignisse in einer Log-Datei. Diese können Sie direkt vom Hauptmenü aus einsehen. Klicken Sie auf **Tools** > **Logs** und wählen Sie dann **Firewall** aus dem Dropdown-Menü **Log**.

Die Log-Dateien sind ein wertvolles Instrument zum Erkennen von Fehlern und zum Aufdecken von versuchten Zugriffen auf das System. Die Log-Dateien der ESET-Personal Firewall enthalten folgende Daten:

- Datum und Uhrzeit des Ereignisses
- Names des Ereignisses
- Quelle
- Zielnetzwerkadresse
- Kommunikationsprotokoll
- Angewendete Regel oder ggf. Name des Wurms
- Betroffene Anwendung
- Benutzer

Eine gründliche Analyse dieser Daten kann zur Erkennung von Sicherheitsbedrohungen beitragen. Viele weitere Faktoren zeigen Ihnen potenzielle Sicherheitslücken auf, damit Sie deren Auswirkungen rechtzeitig eindämmen können: zu häufige Verbindungen von unbekannten Orten, mehrfache Versuche, eine Verbindung aufzubauen, Kommunikation mit unbekannten Anwendungen oder Verwendung ungewöhnlicher Portnummern.

# 9. Web- und E-Mail-Schutz

Klicken Sie im Hauptmenü auf **Einstellungen** > **Web und E-Mail**, um auf den Web- und E-Mail-Schutz zuzugreifen. Sie können von dort aus auch auf ausführliche Einstellungen für die einzelnen Module zugreifen, indem Sie auf **Einstellungen...** klicken.

**Web-Schutz** - Der Web-Schutz überwacht die Kommunikation zwischen Webbrowsern und Remoteservern.

**E-Mail-Client-Schutz** - Der E-Mail-Client-Schutz dient der Überwachung eingehender E-Mails, die mit dem POP3- oder IMAP-Protokoll übertragen werden.

**Phishing-Schutz** - Der Phishing-Schutz blockiert potenzielle Phishing-Angriffe von Websites oder Domänen, die in der Schadsoftware-Datenbank von ESET enthalten sind.

## 9.1 Web-Schutz

Der Web-Schutz dient zur Überwachung von Verbindungen zwischen Webbrowsern und Remote-Servern nach dem HTTP-Protokoll (Hypertext Transfer Protocol).

### 9.1.1 Ports

Auf der Registerkarte **Ports** können Sie die für HTTP-Verbindungen verwendeten Portnummern definieren. In der Standardeinstellung sind die Portnummern 80, 8080 und 3128 vorgegeben.

### 9.1.2 Aktiver Modus

ESET Cyber Security Pro enthält außerdem das Untermenü **Aktiver Modus**, in dem der Prüfungsmodus für Webbrowser festgelegt wird. Der aktive Modus dient der Untersuchung der übertragenen Daten als Ganzes für alle Anwendungen mit Internetzugriff, und zwar unabhängig davon, ob diese Anwendungen als Webbrowser markiert wurden. Ist er nicht aktiviert, wird die Kommunikation der Anwendungen nur Stück für Stück überwacht. Dies verringert die Effizienz der Datenverifizierung, erhöht jedoch die Kompatibilität mit den aufgeführten Anwendungen. Wenn bei seiner Verwendung keine Probleme auftreten, sollten Sie den aktiven Modus aktivieren, indem Sie das Kontrollkästchen neben der gewünschten Anwendung aktivieren.

Wenn eine überwachte Anwendung Daten herunterlädt, werden diese von ESET Cyber Security Pro zunächst in einer temporären Datei gespeichert, jedoch noch nicht an die betreffende Anwendung weitergegeben. Nach Abschluss des Downloads werden die Daten dann auf Schadcode überprüft. Wenn keine Infiltration gefunden wird, werden die Daten an die Anwendung übergeben. Auf diese Weise kann der Datenverkehr überwachter Anwendungen vollständig geprüft werden. Wenn hingegen der passive Modus aktiviert ist, werden die Daten stückweise an die betreffende Anwendung weitergegeben, um Fehler durch Zeitüberschreitung zu vermeiden.

### 9.1.3 URL-Listen

Im Bereich **URL-Listen** können Sie HTTP-Adressen angeben, die gesperrt, zugelassen oder von der Prüfung ausgeschlossen werden sollen. Auf Websites in der Liste der gesperrten Adressen kann nicht zugegriffen werden. Auf Websites in der Liste der ausgeschlossenen Adressen kann zugegriffen werden, ohne dass diese auf Schadcode überprüft werden.

Wenn Sie nur die unter **Zugelassene URL** aufgeführten URL-Adressen zulassen möchten, wählen Sie die Option **URL-Zugriff einschränken**.

Um eine Liste zu aktivieren, wählen Sie die Option **Aktiviert** aus. Wenn Sie benachrichtigt werden möchten, wenn Sie eine Adresse aus der gegenwärtigen Liste eingeben, wählen Sie die Option **Hinweise anzeigen**.

In allen Listen können die Sonderzeichen *(Sternchen) und ?(Fragezeichen) verwendet werden. Das Sternchen steht für eine beliebige Zeichenfolge, das Fragezeichen für ein beliebiges Zeichen. Die Liste der ausgeschlossenen Adressen sollten Sie mit Bedacht zusammenstellen. Geben Sie ausschließlich vertrauenswürdige und sichere Adressen an. Achten Sie außerdem darauf, dass die Zeichen „*“ und „?“ korrekt verwendet werden.

## 9.2 E-Mail-Schutz

Der E-Mail-Schutz dient der Überwachung eingehender E-Mails, die mit dem POP3- oder IMAP-Protokoll übertragen werden. Für die Prüfung eingehender Nachrichten verwendet das Programm alle erweiterten ThreatSense-Prüfmethoden. Die Erkennung von Schadcode findet also noch vor dem Abgleich mit der Signaturdatenbank statt. Die Prüfung des POP3- und IMAP-Datenverkehrs erfolgt unabhängig vom verwendeten E-Mail-Programm.

**ThreatSense-Prüfmodul** - In den erweiterten Prüfeinstellungen

können Sie die zu prüfenden Objekte, die Erkennungsmethoden usw. konfigurieren. Klicken Sie auf **Einstellungen**, um die ausführlichen Prüfeinstellungen anzuzeigen.

An jede E-Mail, die überprüft wurde, kann ein Prüfhinweis angehängt werden. Hierzu können Sie die Option **Prüfhinweise zu E-Mail-Betreff hinzufügen** aktivieren. Auf diese Hinweise sollte sich der Empfänger jedoch nicht unbesehen verlassen, da sie bei problematischen HTML-Nachrichten eventuell verloren gehen oder von manchen Viren auch gefälscht werden können. Die folgenden Optionen stehen zur Verfügung:

**Nie** - Es werden keine Prüfhinweise hinzugefügt.
**Nur bei infizierten E-Mails** - Nur Nachrichten mit Schadsoftware werden als geprüft gekennzeichnet.
**Bei allen geprüften E-Mails** - Es werden Prüfhinweise an alle geprüften E-Mails angehängt.

**Text, der zur Betreffzeile infizierter E-Mails hinzugefügt wird** - Hier können Sie das Betreffpräfix für infizierte E-Mails bearbeiten.

**Prüfhinweise am Ende der E-Mail hinzufügen** - Aktivieren Sie dieses Kontrollkästchen, wenn zu infizierten E-Mails eine Virenwarnung hinzugefügt werden soll. Auf diese Weise können infizierte Nachrichten leicht gefiltert werden. Die Warnung erhöht außerdem die Glaubwürdigkeit beim Empfänger und bietet beim Erkennen einer Infiltration wertvolle Informationen zur Gefährdung durch eine bestimmte E-Mail oder einen Absender.

### 9.2.1 Prüfen von E-Mails per POP3-Protokoll

Das POP3-Protokoll ist das am weitesten verbreitete Protokoll für den Empfang von E-Mails mit einer E-Mail-Client-Anwendung. ESET Cyber Security Pro bietet Schutz für dieses Protokoll unabhängig vom verwendeten E-Mail-Client.

Das Modul für diesen Schutz wird beim Systemstart automatisch gestartet und bleibt danach im Arbeitsspeicher aktiv. Achten Sie darauf, dass das Modul aktiviert ist, damit es richtig arbeiten kann. Die Prüfung von E-Mails per POP3-Protokoll wird automatisch ausgeführt - Sie müssen den E-Mail-Client dazu nicht neu konfigurieren. Standardmäßig wird der gesamte Datenverkehr über Port 110 geprüft; weitere Kommunikationsports können bei Bedarf hinzugefügt werden. Die Portnummern müssen mit einem Komma voneinander getrennt werden.

Wenn die Option **Prüfen von E-Mails per POP3-Protokoll aktivieren** aktiviert ist, wird der gesamte Datenverkehr über POP3 auf Schadsoftware geprüft.

### 9.2.2 Prüfen von E-Mails per IMAP-Protokoll

Das Internet Message Access Protocol (IMAP) ist ein weiteres Internetprotokoll für den Abruf von E-Mails. IMAP bietet gegenüber POP3 einige Vorteile. Beispielsweise können sich mehrere Clients gleichzeitig an demselben Postfach anmelden und die Statusinformationen für Nachrichten (d. h., ob eine Nachricht als gelesen oder ungelesen markiert ist, ob sie beantwortet oder gelöscht wurde) beibehalten. ESET Cyber Security Pro bietet Schutz für dieses Protokoll unabhängig vom verwendeten E-Mail-Client.

Das Modul für diesen Schutz wird beim Systemstart automatisch gestartet und bleibt danach im Arbeitsspeicher aktiv. Achten Sie darauf, dass das Modul aktiviert ist, damit es richtig arbeiten kann. Die Prüfung von E-Mails per IMAP-Protokoll wird automatisch ausgeführt - Sie müssen den E-Mail-Client dazu nicht neu konfigurieren. Standardmäßig wird der gesamte Datenverkehr über Port 143 geprüft; weitere Kommunikationsports können bei Bedarf hinzugefügt werden. Die Portnummern müssen mit einem Komma voneinander getrennt werden.

Wenn die Option **Prüfen von E-Mails per IMAP-Protokoll aktivieren** aktiviert ist, wird der gesamte Datenverkehr über IMAP auf Schadsoftware geprüft.

## 10. Kindersicherung

Im Bereich **Kindersicherung** können Sie die Einstellungen der Kindersicherung konfigurieren. Diese bietet Eltern automatische Mechanismen zum Schutz ihrer Kinder. Ihr Ziel ist es, Kinder und Jugendliche vor Webseiten mit ungeeignetem oder anstößigem Inhalt zu schützen. Mit der Kindersicherung können Sie Webseiten sperren, die möglicherweise jugendgefährdendes Material enthalten. Darüber hinaus haben Eltern die Möglichkeit, den Zugriff auf 27 vordefinierte Website-Kategorien zu sperren.

Ihre Benutzerkonten werden im Fenster **Kindersicherung** angezeigt (**Einstellungen** > **Erweiterte Einstellungen** > **Kindersicherung**). Wählen Sie das Konto aus, für das Sie die Kindersicherung aktivieren möchten. Um eine Schutzebene für das gewählte Konto festzulegen, klicken Sie auf **Einstellungen**. Wenn Sie ein neues Konto erstellen möchten, klicken Sie auf **Hinzufügen**. Dadurch gelangen Sie zurück zur Mac OS-Systemkontoübersicht.

Wählen Sie im Fenster **Kindersicherung einrichten** eins der vordefinierten Profile aus dem Dropdown-Menü **Einstellungsprofil** oder kopieren Sie die Kindersicherungseinstellungen von einem anderen Benutzerkonto. Jedes Profil enthält eine modifizierte Liste der zugelassenen Kategorien. Jede markierte Kategorie gilt als zugelassen. Wenn Sie Ihre Maus auf eine Kategorie bewegen, wird Ihnen eine Liste der Webseiten angezeigt, die in diese Kategorie fallen.

Wenn Sie die Liste **Zugelassene und gesperrte Webseiten** ändern möchten, klicken Sie unten in einem Fenster auf **Einstellungen** und fügen Sie einen Domainnamen zur gewünschten Liste hinzu. Lassen Sie *http://* bei der Eingabe weg. Die Verwendung von Platzhaltern (*) ist nicht notwendig. Wenn Sie nur einen Domainnamen eingeben, sind alle Subdomains darin eingeschlossen. Wenn Sie beispielsweise *google.com* zur Liste **Zugelassene Webseiten** hinzufügen, werden sämtliche Subdomains (*mail.google.com*, *news.google.com*, *maps.google.com* usw.) ebenfalls zugelassen.

**HINWEIS:** Das Sperren bzw. Zulassen einer spezifischen Webseite ist genauer als das Sperren bzw. Zulassen einer ganzen Kategorie von Webseiten.

# 11. Update

Für optimalen Schutz muss ESET Cyber Security Pro regelmäßig aktualisiert werden. Die Updates für die Signaturdatenbank halten das Programm fortlaufend auf dem neuesten Stand.

Über den Punkt **Update** im Hauptmenü können Sie sich den aktuellen Update-Status anzeigen lassen. Sie sehen hier Datum und Uhrzeit des letzten Updates und können feststellen, ob ein Update erforderlich ist. Um ein Update manuell zu starten, klicken Sie auf **Signaturdatenbank aktualisieren**.

Wenn keinerlei Zwischenfälle beim Update-Download auftreten, wird im Update-Fenster der Hinweis **Signaturdatenbank ist auf dem neuesten Stand** angezeigt. Wenn das Update der Signaturdatenbank fehlschlägt, sollten Sie die Update-Einstellungen 16 überprüfen. Die häufigste Fehlerursache sind falsch eingegebene Lizenzdaten (Benutzername/Passwort) oder fehlerhaft konfigurierte Verbindungseinstellungen 22.

Die Versionsnummer der Signaturdatenbank wird hier ebenfalls angezeigt. Diese Nummer ist ein aktiver Link zur ESET-Website, auf der alle Signaturen aufgeführt werden, die bei dem entsprechenden Update hinzugefügt wurden.

**HINWEIS:** Den Benutzernamen und das Passwort erhalten Sie von ESET, nachdem Sie ESET Cyber Security Pro gekauft haben.

## 11.1 Einstellungen für Updates

Zur Anmeldung beim ESET Update-Server verwenden Sie den Benutzernamen und das Passwort, die beim Kauf erzeugt und Ihnen zugestellt wurden.

Um den Testmodus zu aktivieren (d. h. Updates vor ihrer offiziellen Veröffentlichung herunterzuladen), klicken Sie auf **Einstellungen** > **Erweiterte Einstellungen** (oder drücken *cmd+,*) > **Update**, klicken neben **Erweiterte Einstellungen** auf **Einstellungen** und aktivieren das Kontrollkästchen **Testmodus aktivieren**. Der Testmodus sollte nur aktiviert werden, wenn ein frühzeitiges Update verfügbar ist, mit dem ein Problem in ESET Cyber Security Pro behoben wird.

Um die Meldungen im Infobereich der Taskleiste zu deaktivieren, die nach jedem erfolgreichen Update angezeigt werden, aktivieren Sie das Kontrollkästchen **Keinen Hinweis zu erfolgreichem Update anzeigen**.

Um alle vorübergehend gespeicherten Update-Daten zu löschen, klicken Sie auf **Leeren** neben **Update-Cache leeren**. Dies kann helfen, wenn Probleme beim Update auftreten.

## 11.2 So erstellen Sie Update-Tasks

Mit der Option **Signaturdatenbank aktualisieren** können Updates manuell ausgeführt werden. Klicken Sie dazu im Hauptmenü auf **Update**, und wählen Sie im daraufhin angezeigten Dialogfenster die entsprechende Option aus.

Darüber hinaus können Sie Updates auch als geplante Tasks einrichten. Um einen Task zu konfigurieren, klicken Sie auf **Tools** > **Taskplaner**. Standardmäßig sind in ESET Cyber Security Pro folgende Tasks aktiviert:

- **Automatische Updates in festen Zeitabständen**
- **Automatische Updates beim Anmelden des Benutzers**

Diese Update-Tasks können bei Bedarf bearbeitet werden. Neben den standardmäßig ausgeführten Update-Tasks können zusätzliche Update-Tasks mit benutzerdefinierten Einstellungen erstellt werden. Weitere Informationen zum Erstellen und Konfigurieren von Update-Tasks finden Sie im Abschnitt Taskplaner 18.

## 11.3 Upgrade von ESET Cyber Security Pro auf eine neue Version

Um maximalen Schutz zu gewährleisten, ist es wichtig, immer das neueste Build von ESET Cyber Security Pro zu verwenden. Klicken Sie auf **Startseite** im Hauptmenü links, um zu prüfen, ob eine neue Version verfügbar ist. Wenn ein neues Build verfügbar ist, wird eine entsprechende Meldung angezeigt. Klicken Sie auf **Mehr Informationen**, um ein neues Fenster mit der Versionsnummer des neuen Builds und dem Änderungsprotokoll anzuzeigen.

Klicken Sie auf **Ja**, um das aktuelle Build herunterzuladen, oder auf **Jetzt nicht**, um das Fenster zu schließen und das Upgrade später herunterzuladen.

Wenn Sie auf **Ja** geklickt haben, wird die Datei heruntergeladen und in Ihrem Download-Ordner (oder in dem von Ihrem Browser festgelegten Standardordner) abgelegt. Führen Sie nach Abschluss des Downloads die Datei aus und folgen Sie den Installationsanweisungen. Ihr Benutzername und Passwort werden automatisch bei der neuen Installation übernommen. Es wird empfohlen, regelmäßig auf verfügbare Upgrades zu prüfen, insbesondere wenn ESET Cyber Security Pro von einer CD oder DVD installiert wird.

### 11.4 Systemupdates

Die Systemupdatefunktion für Mac OS X ist eine wichtige Komponente zum Schutz des Benutzers vor Schadcode. Zur Gewährleistung des bestmöglichen Schutzes empfehlen wird, die Updates möglichst umgehend zu installieren, sobald sie verfügbar sind. ESET Cyber Security Pro zeigt je nach den von Ihnen festgelegten Einstellungen Benachrichtigungen zu fehlenden Updates an. Sie können diese Benachrichtigungseinstellungen für Updates unter **Einstellungen** > **Erweiterte Einstellungen ...** (oder drücken Sie *cmd+,*) > **Warnungen und Hinweise > Einstellungen...** anpassen. Ändern Sie dazu die Optionen unter **Anzeigebedingungen** neben dem Eintrag **Betriebssystem-Updates**.

- **Alle Updates anzeigen** - Benachrichtigungen werden für alle fehlenden Updates angezeigt.
- **Nur empfohlene Updates anzeigen** - Benachrichtigungen werden nur für empfohlene Updates angezeigt.

Wenn Sie keine Benachrichtigungen zu fehlenden Updates erhalten möchten, deaktivieren Sie das Kontrollkästchen neben **Betriebssystem-Updates**.

Das Benachrichtigungsfenster enthält eine Übersicht der verfügbaren Updates für das Mac OS X-Betriebssystem und für die Anwendungen, die über das native Mac OS X-Tool für Software-Updates aktualisiert werden. Sie können das Update direkt über das Benachrichtigungsfenster ausführen oder über die **Startseite** von ESET Cyber Security Pro, indem Sie hier auf **Fehlendes Update installieren** klicken.

Das Benachrichtigungsfenster enthält den Anwendungsnamen, die Version, die Größe, Eigenschaften (Flags) und zusätzliche Informationen zu den verfügbaren Updates. Die Spalte **Flags** enthält folgende Informationen:

- **[empfohlen]** - Der Hersteller des Betriebssystem empfiehlt die Installation dieses Updates, um die Sicherheit und Stabilität des Systems zu verbessern.
- **[Neustart]** - Nach der Installation ist ein Neustart des Computers erforderlich.
- **[Herunterfahren]** - Der Computer muss heruntergefahren und nach der Installation wieder eingeschaltet werden.

Das Benachrichtigungsfenster zeigt die vom Befehlszeilenwerkzeug 'softwareupdate' abgerufenen Updates an. Die von diesem Werkzeug abgerufenen Updates können sich von den in der Anwendung 'Software Updates' angezeigten Updates unterscheiden. Wenn Sie alle im Fenster 'Fehlende Systemupdates' angezeigten, verfügbaren Updates installieren möchten, einschließlich der nicht in der Anwendung 'Software Updates' angezeigten Updates, verwenden Sie das Befehlszeilenwerkzeug 'softwareupdate'. Weitere Informationen zu diesem Werkzeug finden Sie im Handbuch zu 'softwareupdate', auf das Sie durch Eingabe des Befehls `man softwareupdate` ein einem **Terminal**fenster zugreifen können. Wir empfehlen die Nutzung des Werkzeugs nur für fortgeschrittene Benutzer.

# 12. Tools

Das Menü **Tools** enthält Module zur einfacheren Verwaltung des Programms sowie zusätzliche Optionen für fortgeschrittene Benutzer.

### 12.1 Log-Dateien

Die Log-Dateien enthalten Informationen zu wichtigen aufgetretenen Programmereignissen und geben einen Überblick über erkannte Bedrohungen. Das Erstellen von Logs ist unabdingbar für die Systemanalyse, die Erkennung von Problemen oder Risiken sowie die Fehlerbehebung. Die Logs werden im Hintergrund ohne Eingriffe des Benutzers erstellt. Welche Informationen aufgezeichnet werden, ist abhängig von den aktuellen Einstellungen für die Mindestinformation in Logs. Textnachrichten und Logs können direkt aus ESET Cyber Security Pro heraus angezeigt werden. Das Archivieren von Logs erfolgt ebenfalls direkt über das Programm.

Log-Dateien können über das Hauptfenster von ESET Cyber Security Pro aufgerufen werden, indem Sie auf **Tools** > **Logs** klicken. Wählen Sie in der Liste **Log** im oberen Bereich des Fensters das gewünschte Log aus. Folgende Logs sind verfügbar:

1. **Erkannte Bedrohungen** - Über diese Option können Sie sämtliche Informationen über Ereignisse bezüglich der Erkennung eingedrungener Schadsoftware anzeigen.
2. **Ereignisse** - Diese Option unterstützt Systemadministratoren und Benutzer bei der Behebung von Problemen. Alle von ESET Cyber Security Pro ausgeführten wichtigen Aktionen werden in den Ereignis-Logs aufgezeichnet.
3. **Computer prüfen** - In diesem Log werden die Ergebnisse aller durchgeführten Prüfungen angezeigt. Durch Doppelklicken auf einen Eintrag können Sie Einzelheiten zu der entsprechenden On-Demand-Prüfung anzeigen.
4. **Kindersicherung** - Bei dieser Option werden alle gesperrten Webseiten angezeigt.
5. **Firewall** - Dieses Log enthält die Ergebnisse sämtlicher netzwerkbezogener Ereignisse.

In jedem Abschnitt können die angezeigten Informationen direkt in die Zwischenablage kopiert werden. Dazu wählen Sie die gewünschten Einträge aus und klicken auf **Kopieren**.

#### 12.1.1 Log-Wartung

Die Log-Konfiguration für ESET Cyber Security Pro können Sie aus dem Hauptprogrammfenster aufrufen. Klicken Sie auf **Einstellungen** > **Erweiterte Einstellungen ...** (oder drücken Sie *cmd+,*) > **Log-Dateien**. Für Log-Dateien können die folgenden Einstellungen vorgenommen werden:

- **Alte Log-Einträge automatisch löschen** - Log-Einträge, die älter als die angegebene Anzahl Tage sind, werden automatisch gelöscht.
- **Log-Dateien automatisch optimieren** - Die Logs werden beim Erreichen des vordefinierten Fragmentierungsgrads automatisch optimiert.

Um den **Standardfilter für Log-Einträge** zu konfigurieren, klicken Sie auf **Bearbeiten...** und aktivieren/deaktivieren die einzelnen Log-Typen je nach Bedarf.

### 12.1.2 Log-Filter

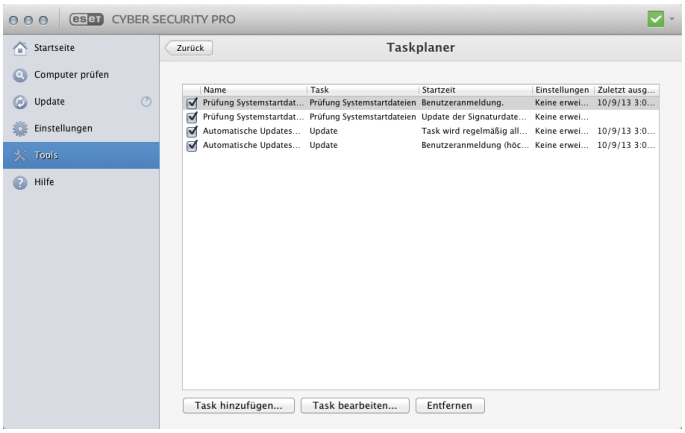
In den Logs werden Informationen über wichtige Systemereignisse gespeichert. Mit dem Log-Filter können Sie sich gezielt Einträge zu einer bestimmten Ereignisart anzeigen lassen.

Die gängigsten Eintragsarten sind:

- **Kritische Warnungen** - Kritische Systemfehler (z. B. „Virenschutz konnte nicht gestartet werden“)
- **Fehler** - Fehler wie z. B. *„Fehler beim Herunterladen einer Datei“* und kritische Fehler
- **Warnungen** - Warnmeldungen
- **Informationen** - Meldungen wie erfolgreiche Updates, Warnungen usw.
- **Diagnosedaten** - Alle bisher genannten Einträge sowie Informationen, die für die Feineinstellung des Programms erforderlich sind.

## 12.2 Taskplaner

Um den Taskplaner zu öffnen, klicken Sie im Hauptmenü von ESET Cyber Security Pro unter **Tools** auf **Taskplaner**. Der Taskplaner umfasst eine Liste aller geplanten Tasks sowie deren Konfigurationseigenschaften, inklusive des vordefinierten Datums, der Uhrzeit und des verwendeten Prüfprofils.




Der Taskplaner verwaltet und startet geplante Tasks mit vordefinierter Konfiguration und voreingestellten Eigenschaften. Konfiguration und Eigenschaften enthalten Informationen wie Datum und Uhrzeit und bestimmte Profile, die bei Ausführung des Tasks verwendet werden.

Standardmäßig werden im Taskplaner die folgenden Tasks angezeigt:

- Log-Wartung (nach Aktivieren der Option **System-Tasks anzeigen** in den Taskplaner-Einstellungen)
- Prüfung Systemstartdateien nach Anmeldung des Benutzers
- Prüfung Systemstartdateien nach Update der Signaturdatenbank
- Automatische Updates in festen Zeitabständen
- Automatische Updates beim Anmelden des Benutzers

Um die Konfiguration eines vorhandenen Standardtasks oder eines benutzerdefinierten Tasks zu ändern, halten Sie die Ctrl-Taste gedrückt, klicken auf den Task und dann auf **Bearbeiten**. Alternativ können Sie den Task, den Sie ändern möchten, auswählen und dann auf **Task bearbeiten** klicken.

### 12.2.1 Erstellen von Tasks

Zum Erstellen eines Tasks im Taskplaner klicken Sie auf **Task hinzufügen...** oder halten die Strg-Taste gedrückt, klicken auf das leere Feld und wählen dann im Kontextmenü die Option **Hinzufügen...**. Es gibt fünf Arten von Tasks:

- **Anwendung starten**
- **Update**
- **Log-Wartung**
- **On-Demand-Prüfung**
- **Prüfung Systemstartdateien**

**HINWEIS:** Wenn Sie **Anwendung ausführen** auswählen, können Sie Programme mit dem Systembenutzer „nobody“ („niemand“) ausführen. Die Berechtigungen zum Ausführen von Anwendungen über den Taskplaner werden über Mac OS X definiert.

Im nachfolgenden Beispiel wird über den Taskplaner ein neues Update-Task hinzugefügt (Updates stellen die am häufigsten geplanten Tasks dar):

1. Wählen Sie im Dropdownmenü **Geplanter Task** die Option **Update**.
2. Geben Sie im Feld **Taskname** den Namen des Tasks ein.
3. Wählen Sie in der Liste **Task ausführen** das gewünschte Ausführungsintervall. Je nach ausgewähltem Intervall werden Sie aufgefordert, verschiedene Update-Parameter festzulegen. Bei der Auswahl **Benutzerdefiniert** werden Sie aufgefordert, Datum und Uhrzeit im cron-Format anzugeben (nähere Informationen siehe Abschnitt Erstellen eines benutzerdefinierten Tasks 18).
4. Im nächsten Schritt legen Sie eine Aktion für den Fall fest, dass der Task zur geplanten Zeit nicht ausgeführt oder abgeschlossen werden kann.
5. Im letzten Schritt wird eine Übersicht der Einstellungen zum geplanten Task angezeigt. Klicken Sie auf **Fertig stellen**. Der neue geplante Task wird der Liste der aktuellen Tasks hinzugefügt.

Einige Tasks sind für die ordnungsgemäße Funktion des Systems unerlässlich und standardmäßig in ESET Cyber Security Pro enthalten. Diese System-Tasks sollten nicht modifiziert werden. Die Anzeige ist standardmäßig ausgeschaltet. Zur Anzeigen dieser Tasks klicken Sie im Hauptmenü auf **Einstellungen** > **Erweiterte Einstellungen ...** (oder drücken *cmd+,*) > **Taskplaner** und aktivieren die Option **System-Tasks anzeigen**.

### 12.2.2 Erstellen von benutzerdefinierten Tasks

Datum und Uhrzeit von Tasks des Typs **Benutzerdefiniert** müssen im cron-Langformat mit Jahr angegeben werden (Zeichenfolge aus 6 Feldern, jeweils getrennt durch ein Whitespace-Zeichen):

```
Minute(0-59) Stunde(0-23) Tag(1-31) Monat(1-12) Jahr(1970-2099) Wochentag(0-7)(Sonntag = 0 oder 7)
```

Beispiel:

```
30 6 22 3 2012 4
```

In cron-Ausdrücken werden die folgenden Sonderzeichen unterstützt:

- Sternchen (*) - Steht für alle möglichen Werte des betreffenden Felds. Beispiel: Sternchen im dritten Feld (Tag) = jeder Tag im Monat

- Bindestrich (-) - Definition von Zeiträumen, z. B. `3-9`
- Komma (,) - Trennt mehrere Einträge einer Liste, z. B. `1,3,7,8`
- Schrägstrich (/) - Definition von Intervallen in Zeiträumen. Beispiel: `3-28/5` im dritten Feld (Tag) = am 3. des Monats und anschließend alle 5 Tage

Textbezeichnungen für Tage (Monday-Sunday) und Monate ( January-December) werden nicht unterstützt.

**HINWEIS:** Werden sowohl Tag als auch Wochentag angegeben, so wird der Befehl nur ausgeführt, wenn beide Bedingungen erfüllt sind.

## 12.3 Quarantäne

Die Hauptaufgabe der Quarantäne ist die sichere Verwahrung infizierter Dateien. Dateien sollten in die Quarantäne verschoben werden, wenn sie nicht gesäubert werden können, wenn es nicht sicher oder ratsam ist, sie zu löschen, oder wenn sie von ESET Cyber Security Pro fälschlicherweise erkannt worden sind.

Sie können beliebige Dateien gezielt in die Quarantäne verschieben. Geschehen sollte dies bei Dateien, die sich verdächtig verhalten, bei der Virenprüfung jedoch nicht erkannt werden. Dateien, die in die Quarantäne verschoben wurden, können zur Analyse an das ESET-Virenlabor übermittelt werden.

Die Dateien im Quarantäneordner können in einer Tabelle angezeigt werden, die Datum und Uhrzeit der Quarantäne, den Pfad zum ursprünglichen Speicherort der infizierten Datei, ihre Größe in Byte, einen Grund (Hinzugefügt durch Benutzer...) und die Anzahl der Bedrohungen (z. B. bei Archiven, in denen an mehreren Stellen Schadcode erkannt wurde) enthält. Das Quarantäneverzeichnis (*/Library/Application Support/Eset/esets/cache/quarantine*) verbleibt auch nach der Deinstallation von ESET Cyber Security Pro im System. Die Quarantänedateien werden sicher verschlüsselt gespeichert und können nach der Reinstallation von ESET Cyber Security Pro wiederhergestellt werden.

### 12.3.1 Quarantäne für Dateien

ESET Cyber Security Pro kopiert gelöschte Dateien automatisch in den Quarantäneordner (sofern diese Option nicht im Warnfenster deaktiviert wurde). Auf Wunsch können Sie beliebige verdächtige Dateien manuell in die Quarantäne verschieben, indem Sie auf **Quarantäne** klicken. Alternativ kann auch das Kontextmenü zu diesem Zweck verwendet werden: Halten Sie die Ctrl-Taste gedrückt, klicken Sie in das leere Feld, wählen Sie **Quarantäne**, wählen Sie die Datei, die in die Quarantäne verschoben werden soll, und klicken Sie auf **Öffnen**.

### 12.3.2 Wiederherstellen aus Quarantäne

Dateien aus der Quarantäne können auch an ihrem ursprünglichen Speicherort wiederhergestellt werden. Verwenden Sie dazu die Schaltfläche **Wiederherstellen**. Sie können die Funktion auch über das Kontextmenü aufrufen. Halten Sie dazu die Ctrl-Taste gedrückt, klicken Sie im Fenster **Quarantäne** auf die gewünschte Datei und wählen Sie dann **Wiederherstellen**. Das Kontextmenü enthält außerdem die Option **Wiederherstellen nach**, mit der Dateien an einem anderen als ihrem ursprünglichen Speicherort wiederhergestellt werden können.

### 12.3.3 Einreichen von Dateien aus der Quarantäne

Wenn Sie eine verdächtige, nicht vom Programm erkannte Datei in die Quarantäne verschoben haben oder wenn eine Datei fälschlich als infiziert eingestuft wurde (etwa durch die heuristische Analyse des Codes) und infolgedessen in den Quarantäneordner verschoben wurde, senden Sie die Datei zur Analyse an das ESET-Virenlabor. Um eine Datei aus der Quarantäne zu senden, halten Sie die Ctrl-Taste gedrückt, klicken Sie auf die Datei und wählen Sie aus dem Kontextmenü die Option **Datei zur Analyse einreichen**.

## 12.4 Ausgeführte Prozesse

Die Liste **Ausgeführte Prozesse** zeigt die auf Ihrem Computer ausgeführten Prozesse an. ESET Cyber Security Pro liefert detaillierte Informationen zu den ausgeführten Prozessen, um Benutzern den Schutz der ESET Live Grid-Technologie zu bieten.

- **Prozess** - Name des aktuell auf Ihrem Computer ausgeführten Prozesses. Sie können sämtliche ausgeführten Prozesse auch in der Aktivitätsanzeige (*/Programme/Dienstprogramme*) anzeigen.
- **Risikostufe** - In den meisten Fällen weisen ESET Cyber Security Pro und die ESET Live Grid-Technologie den Objekten (Dateien, Prozesse usw.) eine Risikostufe zu. Dies erfolgt unter Einsatz einer Reihe heuristischer Regeln, die die Eigenschaften des Objekts untersuchen und auf dieser Grundlage den Verdacht auf Schadcode abwägen. Den Objekten wird auf Grundlage dieser heuristischen Regeln eine Risikostufe zugewiesen. Bekannte Anwendungen, die grün markiert und bekanntermaßen keinen Schadcode enthalten (Positivliste), werden von der Prüfung ausgeschlossen. Dies sorgt für eine schnellere On-Demand- und Echtzeit-Prüfung. Eine als unbekannt eingestufte Anwendung (gelb) enthält nicht unbedingt Schadcode. Meist handelt es sich einfach um eine neuere Anwendung. Wenn Sie sich nicht sicher sind, ob die Datei Schadcode enthält, können Sie sie zur Analyse an das ESET-Virenlabor senden. Wenn sich herausstellt, dass die Datei Schadcode enthält, wird ihre Erkennung in eines der zukünftigen Updates integriert.
- **Anzahl Benutzer** - gibt die Anzahl der Benutzer an, die eine bestimmte Anwendung verwenden. Diese Information wird durch die ESET Live Grid-Technologie erfasst.
- **Erkennungszeit** - gibt an, wann die Anwendung von der ESET Live Grid-Technologie erkannt wurde.
- **Anwendungspaket-ID** - Name des Herstellers oder des Anwendungsprozesses.

Wenn Sie auf einen Prozess klicken, werden am unteren Bildschirmrand folgende Informationen angezeigt:

- **Datei** - Speicherort der Anwendung auf Ihrem Computer
- **Dateigröße** - physikalische Größe der Datei auf dem Datenträger
- **Dateibeschreibung** - Dateieigenschaften auf Grundlage der Beschreibung vom Betriebssystem
- **Anwendungspaket-ID** - Name des Herstellers oder des Anwendungsprozesses
- **Dateiversion** - Informationen vom Herausgeber der Anwendung
- **Produktname** - Anwendungs- und/oder Firmenname

## 12.5 Live Grid

Dank des Live Grid-Frühwarnsystems erhält ESET unmittelbar und fortlaufend aktuelle Informationen zu neuen Infiltrationen. Das Live Grid-Frühwarnsystem funktioniert in zwei Richtungen, hat jedoch nur einen Zweck: die Verbesserung des Schutzes, den wir Ihnen bieten. Die einfachste Möglichkeit, neue Bedrohungen zu erkennen, sobald sie in Erscheinung treten, besteht darin, so viele Kunden wie möglich als Virenscouts einzusetzen. Als Benutzer haben Sie zwei Möglichkeiten:

1. Sie können sich entscheiden, das Live Grid-Frühwarnsystem nicht zu aktivieren. Es steht Ihnen dennoch der volle Funktionsumfang der Software zur Verfügung, und Sie erhalten auch in diesem Fall den bestmöglichen Schutz.
2. Sie können das Live Grid-Frühwarnsystem so konfigurieren, dass Informationen über neue Bedrohungen und Fundstellen von gefährlichem Code übermittelt werden. Die Informationen bleiben anonym. Diese Informationen können zur detaillierten Analyse an ESET gesendet werden. Durch die Untersuchung dieser Bedrohungen kann ESET seine Datenbanken ergänzen und die Fähigkeit seiner Software zur Erkennung von Bedrohungen verbessern.

Das Live Grid-Frühwarnsystem sammelt Daten über neue Bedrohungen, die auf Ihrem Computer erkannt wurden. Dazu können auch Proben oder Kopien einer Datei gehören, in der eine Bedrohung aufgetreten ist, der Pfad zu dieser Datei, der Dateiname, Datum und Uhrzeit, der Prozess, über den die Bedrohung auf Ihrem Computer in Erscheinung getreten ist, und Informationen zum Betriebssystem des Computers.

Auch wenn es möglich ist, dass das ESET-Virenlabor auf diese Weise gelegentlich einige Informationen über Sie oder Ihren Computer erhält (zum Beispiel Benutzernamen in einem Verzeichnispfad usw.), werden diese Daten für keinen anderen Zweck als zur Verbesserung der unmittelbaren Reaktion auf neue Bedrohungen verwendet.

Zum Zugriff auf die Live Grid-Einrichtung klicken Sie im Hauptmenü auf **Einstellungen** > **Erweiterte Einstellungen ...** (oder *cmd+,* drücken) > **Live Grid**. Wählen Sie **Live Grid-Frühwarnsystem aktivieren** aus, um Live Grid zu aktivieren. Klicken Sie dann neben **Erweiterte Einstellungen** auf **Einstellungen...**.

### 12.5.1 Live Grid-Einstellungen

Standardmäßig ist ESET Cyber Security Pro so konfiguriert, dass verdächtige Dateien zur weiteren Analyse an das ESET-Virenlabor gesendet werden. Wenn Sie solche Dateien nicht automatisch einreichen möchten, deaktivieren Sie die Option **Verdächtige Dateien einreichen**.

Wenn Sie eine verdächtige Datei finden, können Sie sie zur Analyse an unser Virenlabor einreichen. Klicken Sie hierzu im Hauptprogrammfenster auf **Tools** > **Datei zur Analyse einreichen**. Sollte dabei schädlicher Code zutage treten, wird dieser beim nächsten Update der Signaturdatenbank berücksichtigt.

**Anonymisierte statistische Daten einreichen** - Das ESET Live Grid-Frühwarnsystem erfasst anonyme Informationen zu Ihrem Computer in Bezug auf neu erkannte Bedrohungen. Erfasst werden der Name der Bedrohung, Datum und Uhrzeit der Erkennung, die Versionsnummer des ESET Security-Produkts sowie Versionsdaten und die Regionaleinstellung des Betriebssystems. Die Statistikdaten werden normalerweise einmal oder zweimal täglich an ESET übermittelt.

Beispiel für ein typisches Statistikpaket:

```
# utc_time=2005-04-14 07:21:28
# country="Slovakia"
# language="ENGLISH"
# osver=9.5.0
# engine=5417
# components=2.50.2
# moduleid=0x4e4f4d41
# filesize=28368
# filename=Users/UserOne/Documents/Incoming/
rdgFR1463[1].zip
```

**Ausschlussfilter** – Über diese Option können Sie bestimmte Dateitypen vom Senden ausschließen. Hier können Dateien eingetragen werden, die eventuell vertrauliche Informationen enthalten, wie zum Beispiel Textdokumente oder Tabellen. Die üblichsten Dateitypen sind bereits in der Standardeinstellung in die Liste eingetragen (.doc, .rtf usw.). Sie können der Ausschlussliste weitere Dateitypen hinzufügen.

**E-Mail-Adresse für Rückfragen (optional)** - Ihre E-Mail-Adresse kann dazu verwendet werden, Sie bei Rückfragen zu kontaktieren. Bitte beachten Sie, dass Sie nur dann eine Antwort von ESET erhalten, wenn weitere Informationen von Ihnen benötigt werden.

## 12.6 ESET Social Media Scanner

ESET Social Media Scanner ist eine Anwendung zum Schutz vor Schadcode, der über soziale Netzwerke übertragen wird. ESET Social Media Scanner überwacht neue Inhalte in sozialen Medien (beispielsweise Pinnwandeinträge mit Links oder Medien in Facebook) und sucht mittels automatischer oder On-Demand-Prüfung nach Schadcode. Die Prüfergebnisse werden dem Benutzer über eine Nachricht in der Anwendung, eine E-Mail oder einen Kommentar zum infizierten Objekt gemeldet. Als zusätzliche Hilfe beim Schutz vor Bedrohungen werden auf der Pinnwand des Benutzers wöchentliche Statistiken eingefügt. ESET Social Media Scanner ist unabhängig von anderen ESET-Sicherheitsprodukten und völlig kostenlos.

Klicken Sie im Hauptmenü von ESET Cyber Security Pro auf **Tools** > **ESET Social Media Scanner**, um die ESET Social Media Scanner-Webseite zu öffnen und die Anwendung herunterzuladen.

# 13. Benutzeroberfläche

Über die Konfigurationsoptionen für die Benutzeroberfläche können Sie die Arbeitsumgebung an Ihre Anforderungen anpassen. Diese Optionen sind unter **Einstellungen** > **Erweiterte Einstellungen ...** (oder *cmd+,* drücken) > **Schnittstelle** verfügbar.

Um das ESET Cyber Security Pro-Startbild beim Programmstart zu aktivieren, aktivieren Sie die Option **Startbild anzeigen**.

Die Option **Anwendung in Dock anzeigen** bewirkt, dass das ESET Cyber Security Pro-Symbol ⓔ im Mac OS-Dock angezeigt wird und dass Sie mit der Tastenkombination *cmd-tab* zwischen ESET Cyber Security Pro und anderen geöffneten Anwendungen wechseln können. Die Änderungen werden beim nächsten Start von ESET Cyber Security Pro (in der Regel nach einem Neustart des Computers) wirksam.

Wenn Sie die Option **Standardmenü verwenden** aktivieren, können Sie bestimmte Tastaturbefehle 6 verwenden und Standardmenüeinträge in der Mac OS-Menüleiste (oben am Bildschirm) anzeigen.

Um QuickInfos für bestimmte Optionen in ESET Cyber Security Pro anzuzeigen, aktivieren Sie **QuickInfo anzeigen**.

Wenn **Versteckte Dateien anzeigen** aktiviert ist, können Sie im Einstellungsbereich **Zu prüfende Objekte** der Funktion **Computer prüfen** auch versteckte Dateien sehen und diese auswählen.

## 13.1 Warnungen und Hinweise

Im Bereich **Warnungen und Hinweise** können Sie konfigurieren, wie Warnungen und Systemhinweise in ESET Cyber Security Pro behandelt werden.

Wenn Sie die Option **Warnungen anzeigen** deaktivieren, werden keinerlei Warnfenster angezeigt. Dies ist nur in bestimmten Situationen sinnvoll. Für die meisten Benutzer empfiehlt es sich, die Standardeinstellung (aktiviert) beizubehalten.

Wenn Sie die Option **Hinweise auf dem Desktop anzeigen** aktivieren, werden Warnfenster, die keinen Benutzereingriff erfordern, auf dem Desktop angezeigt (standardmäßig oben rechts auf dem Bildschirm). Wie lang solche Hinweise erscheinen, können Sie über den Wert **Hinweise automatisch schließen nach** X **Sekunden** festlegen.

Wenn beim Betrieb von Anwendungen im Vollbildmodus nur Hinweise angezeigt werden sollen, die ein Eingreifen des Benutzers erfordern, aktivieren Sie die Option **Vollbildmodus aktivieren**. Dies ist praktisch für Präsentationen, Spiele oder andere Anwendungen, die die gesamte Bildschirmfläche benötigen.

### 13.1.1 Erweiterte Einstellungen für Warnungen und Hinweise

Bei neuen Programmversionen und Betriebssystem-Updates, beim Deaktivieren bestimmter Programmkomponenten, beim Löschen von Logs usw. werden in ESET Cyber Security Pro Warn- und Hinweisfenster angezeigt. Diese können Sie mit Wirkung für die Zukunft unterdrücken, indem Sie im jeweiligen Dialogfenster die Option **Dialogfenster nicht mehr anzeigen** aktivieren.

Unter **Liste der Dialogfenster** (**Einstellungen** > **Erweiterte Einstellungen** > **Warnungen und Hinweise** > **Einstellungen**) finden Sie eine Liste all dieser Warn- und Hinweisfenster in ESET Cyber Security Pro. Mit den Kontrollkästchen neben **Hinweisname** können Sie diese Hinweise einzeln aktivieren oder unterdrücken. Außerdem können Sie **Anzeigebedingungen** für Hinweise zu neuen Programmversionen und Betriebssystem-Updates definieren.

## 13.2 Berechtigungen

Die Einstellungen von ESET Cyber Security Pro können im Hinblick auf die Sicherheitsrichtlinien Ihres Unternehmens von großer Wichtigkeit sein. Unbefugte Änderungen können die Stabilität und den Schutz Ihres Systems gefährden. Aus diesem Grund können Sie festlegen, welche Benutzer zum Bearbeiten der Programmkonfiguration berechtigt sind.

Zum Festlegen der privilegierten Benutzer klicken Sie auf **Einstellungen** > **Erweiterte Einstellungen …** (oder drücken *cmd+,*) > **Berechtigungen**.

Maßgeblich für einen wirksamen Schutz Ihres Systems sind die korrekten Einstellungen des Programms. Bei unzulässigen Änderungen können wichtige Daten verloren gehen. Um die Liste der privilegierten Benutzer einzurichten, wählen Sie die gewünschten Benutzer links in der Liste **Benutzer** aus und klicken auf **Hinzufügen**. Um alle Benutzer anzuzeigen, wählen Sie die Option **Alle Benutzer anzeigen**. Um einen Benutzer zu entfernen, wählen Sie ihn in der Liste **Privilegierte Benutzer** rechts aus und klicken auf **Entfernen**.

**HINWEIS:** Wenn die Liste der privilegierten Benutzer leer ist, können alle Systembenutzer die Programmeinstellungen bearbeiten.

## 13.3 Kontextmenü

Die Kontextmenü-Integration kann unter **Einstellungen** > **Erweiterte Einstellungen …** (oder *cmd+,* drücken) > **Kontextmenü** durch Auswahl der Option **In Kontextmenü integrieren** aktiviert werden. Die Änderungen werden nach dem Abmelden bzw. einem Neustart des Computers wirksam. Die Optionen des Kontextmenü werden im **Finder**-Fenster angezeigt, wenn Sie bei gedrückter STRG-Taste auf eine beliebige Datei klicken.

# 14. Allgemein

## 14.1 Einstellungen importieren/exportieren

Konfigurationen für ESET Cyber Security Pro können unter **Einstellungen** im- bzw. exportiert werden.

Die Optionen Import und Export verwenden Archivdateien zum Speichern der Konfiguration. Diese Funktionen sind nützlich, wenn Sie die aktuelle Konfiguration von ESET Cyber Security Pro für eine spätere Verwendung sichern möchten. Die Exportfunktion bietet sich auch für Benutzer an, die ihre bevorzugte Konfiguration von ESET Cyber Security Pro auf mehreren Systemen verwenden möchten. Um die gewünschten Einstellungen zu übernehmen, wird die Konfigurationsdatei einfach importiert.

### 14.1.1 Einstellungen importieren

Um eine Konfiguration zu importieren, klicken Sie im Hauptmenü auf **Einstellungen** > **Einstellungen importieren/exportieren** und wählen Sie die Option **Einstellungen importieren**. Geben Sie den Namen der Konfigurationsdatei ein oder klicken Sie auf **Durchsuchen**, um die Konfigurationsdatei zu suchen, die Sie importieren möchten.

### 14.1.2 Einstellungen exportieren

Um eine Konfiguration zu exportieren, klicken Sie im Hauptmenü auf **Einstellungen** > **Einstellungen importieren/exportieren**. Wählen Sie die Option **Einstellungen exportieren** und geben Sie den Namen der Konfigurationsdatei ein. Suchen Sie mithilfe des Browsers einen Speicherort auf Ihrem Computer aus, an dem Sie die Konfigurationsdatei speichern möchten.

## 14.2 Einstellungen für Proxyserver

Die Proxyserver-Einstellungen lassen sich unter **Einstellungen** > **Erweiterte Einstellungen** (oder *cmd+*, drücken) > **Proxyserver** konfigurieren. So legen Sie die allgemeinen Proxyserver-Einstellungen für alle Funktionen von ESET Cyber Security Pro fest. Die hier definierten Parameter werden von allen Modulen verwendet, die eine Verbindung zum Internet erfordern. ESET Cyber Security Pro unterstützt die Authentifizierungsarten „Basic Authentication“ und „NTLM“ (NT LAN Manager).

Um die Proxyserver-Einstellungen für diese Ebene festzulegen, aktivieren Sie das Kontrollkästchen **Proxyserver verwenden** und geben im Feld **Proxyserver** die entsprechende IP-Adresse bzw. URL ein. Geben Sie dann im Feld **Port** den Port an, über den Verbindungen auf dem Proxyserver eingehen (standardmäßig 3128).

Wenn der Proxyserver eine Authentifizierung benötigt, aktivieren Sie das Kontrollkästchen **Proxyserver erfordert Authentifizierung** und geben einen gültigen **Benutzernamen** sowie das entsprechende **Passwort** ein.

# 15. Glossar

## 15.1 Arten von Infiltrationen

Bei Schadsoftware handelt es sich um bösartige Software, die versucht, in einen Computer einzudringen und/oder auf einem Computer Schaden anzurichten.

### 15.1.1 Viren

Bei einem Computervirus handelt es sich um eingedrungene Schadsoftware, die Dateien auf Ihrem Computer beschädigt. Ihren Namen haben sie nicht umsonst mit den Viren aus der Biologie gemein. Schließlich verwenden sie ähnliche Techniken, um sich von einem zum anderen Computer auszubreiten.

Computerviren greifen hauptsächlich ausführbare Dateien, Skripte und Dokumente an. Um sich zu vermehren, hängt sich ein Virus mit seinem „Körper“ an das Ende einer Zieldatei. Und so funktioniert ein Computervirus: Durch Ausführung der infizierten Datei wird der Virus aktiviert (noch bevor die eigentliche Anwendung gestartet wird) und führt seine vordefinierte Aufgabe aus. Erst dann wird die eigentliche Anwendung gestartet. Ein Virus kann einen Computer also nur dann infizieren, wenn der Benutzer (versehentlich oder absichtlich) das bösartige Programm ausführt oder öffnet.

Computerviren unterscheiden sich nach Art und Schweregrad der durch sie verursachten Schäden. Einige von ihnen sind aufgrund ihrer Fähigkeit, Dateien von der Festplatte gezielt zu löschen, äußerst gefährlich. Andererseits gibt es aber auch Viren, die keinen Schaden verursachen. Ihr einziger Zweck besteht darin, den Benutzer zu verärgern und die technischen Fähigkeiten ihrer Urheber unter Beweis zu stellen.

Viren werden (im Vergleich zu Trojanern oder Spyware) immer seltener, da sie keinen kommerziellen Nutzen für ihre Urheber haben. Außerdem wird der Begriff „Virus“ oft fälschlicherweise für alle Arten von Schadsoftware verwendet. Heute setzt sich mehr und mehr der neue, treffendere Ausdruck „Malware“ (engl. bösartige Software) durch.

Wenn Ihr Computer mit einem Virus infiziert wurde, ist es notwendig, den Originalzustand der infizierten Dateien wiederherzustellen - das heißt, den Schadcode mithilfe eines Virenschutzprogrammes daraus zu entfernen.

### 15.1.2 Würmer

Bei einem Computerwurm handelt es sich um ein Programm, das Schadcode enthält, der Hostcomputer angreift und sich über Netzwerke verbreitet. Der grundlegende Unterschied zwischen Viren und Würmern besteht darin, dass Würmer in der Lage sind, sich selbstständig zu vermehren und zu verbreiten. Sie sind unabhängig von Hostdateien (oder Bootsektoren). Würmer verbreiten sich über die E-Mail-Adressen in Ihrer Kontaktliste oder nutzen Sicherheitslücken von Anwendungen in Netzwerken.

Daher sind Würmer wesentlich funktionsfähiger als Computerviren. Aufgrund der enormen Ausdehnung des Internets können sich Würmer innerhalb weniger Stunden über den gesamten Globus verbreiten - manchmal sogar schon in wenigen Minuten. Da sich Würmer unabhängig und rasant vermehren können, sind sie gefährlicher als andere Arten von Schadsoftware.

Ein innerhalb eines Systems aktivierter Wurm kann eine Reihe von Unannehmlichkeiten verursachen: Er kann Dateien löschen, die Systemleistung beeinträchtigen oder Programme deaktivieren. Aufgrund ihrer Beschaffenheit können Würmer als Transportmedium für andere Arten von Schadcode fungieren.

Wurde Ihr Computer mit einem Wurm infiziert, empfiehlt es sich, alle betroffenen Dateien zu löschen, da sie höchstwahrscheinlich Schadcode enthalten.

### 15.1.3 Trojaner

Trojaner galten früher als eine Klasse von Schadprogrammen, die sich als nützliche Anwendungen tarnen, um den Benutzer zur Ausführung zu verleiten. Heute müssen sich Trojaner nicht mehr tarnen. Ihr einzige Absicht besteht darin, sich möglichst leicht Zugang zu einem System zu verschaffen, um dort den gewünschten Schaden anzurichten. Der Ausdruck „Trojaner“ ist zu einem sehr allgemeinen Begriff geworden, der jegliche Form von Schadsoftware beschreibt, die nicht einer bestimmten Kategorie zugeordnet werden kann.

Aus diesem Grund wird die Kategorie „Trojaner“ oft in mehrere Gruppen unterteilt.

- Downloader - Ein bösartiges Programm zum Herunterladen von Schadsoftware aus dem Internet.
- Dropper - Trojaner, der auf angegriffenen Computern weitere Schadsoftware absetzt („droppt“).
- Backdoor - Anwendung, die Angreifern Zugriff auf ein System verschafft, um es zu kontrollieren.
- Keylogger - Programm, das die Tastenanschläge eines Benutzers aufzeichnet und die Informationen an Angreifer sendet.
- Dialer - Dialer sind Programme, die Verbindungen zu teuren Einwahlnummern herstellen. Dass eine neue Verbindung erstellt wurde, ist für den Benutzer nahezu unmöglich festzustellen. Dialer sind nur eine Gefahr für Benutzer von Einwahlmodems. Diese werden allerdings nur noch selten eingesetzt.
- Trojaner treten häufig in Form von ausführbaren Dateien auf. Wenn auf Ihrem Computer eine Datei als Trojaner identifiziert wird, sollte diese gelöscht werden, da sie mit hoher Wahrscheinlichkeit Schadcode enthält.

### 15.1.4 Rootkits

Rootkits sind Schadprogramme, die Angreifern aus dem Internet unbegrenzten Zugriff auf ein System ermöglichen und gleichzeitig ihre Präsenz verbergen. Nach dem Eindringen und Installieren in einem System (üblicherweise durch Ausnutzen von Sicherheitslücken) nutzen Rootkits Funktionen im Betriebssystem, um nicht von Antivirenprogrammen erkannt zu werden: Sie verschleiern Prozesse und Dateien. Aus diesem Grund ist es fast unmöglich, sie mit herkömmlichen Prüfmethoden zu erkennen.

Zum Schutz vor Rootkits gibt es zwei Erkennungsstufen:

1. Beim versuchten Zugriff auf ein System - sie sind noch nicht präsent und daher inaktiv. Die meisten Antivirensysteme sind in der Lage, Rootkits zu diesem Zeitpunkt zu beseitigen (vorausgesetzt, sie erkennen diese Dateien als infiziert).
2. Rootkits, die sich von üblichen Prüfungen verbergen

### 15.1.5 Adware

Adware ist eine Abkürzung für durch Werbung (engl. Advertising) unterstützte Software. In diese Kategorie fallen Programme, in denen Werbung angezeigt wird. Adware-Anwendungen öffnen häufig in Internetbrowsern neue Popup-Fenster mit Werbung oder ändern die Startseite des Browsers. Adware gehört oftmals zu Freeware-Programmen, damit die Freeware-Entwickler auf diesem Weg die Entwicklungskosten ihrer (gewöhnlich nützlichen) Anwendungen decken können.

Adware selbst ist nicht gefährlich. Allerdings werden die Benutzer mit Werbung belästigt. Bedenklich ist aber, dass Adware auch dazu dienen kann, Daten zu sammeln (wie es bei Spyware der Fall ist).

Wenn Sie sich dafür entscheiden, ein Freeware-Produkt zu verwenden, sollten Sie bei der Installation besonders aufmerksam sein. Die meisten Installationsprogramme benachrichtigen Sie über die Installation eines zusätzlichen Adware-Programms. In vielen Fällen ist es möglich, diesen Teil der Installation abzubrechen und das Programm ohne Adware zu installieren.

In einigen Fällen lassen sich Programme jedoch nicht ohne die Adware installieren, oder nur mit eingeschränktem Funktionsumfang. Das bedeutet, dass Adware häufig ganz „legal“ auf das System zugreift, da sich die Benutzer damit einverstanden erklärt haben. In diesem Fall gilt: Vorsicht ist besser als Nachsicht. Wenn auf Ihrem Computer eine Datei als Adware identifiziert wird, sollte diese gelöscht werden, da sie mit hoher Wahrscheinlichkeit Schadcode enthält.

### 15.1.6 Spyware

Der Begriff „Spyware“ fasst alle Anwendungen zusammen, die vertrauliche Informationen ohne das Einverständnis/Wissen des Benutzers versenden. Diese Programme verwenden Überwachungsfunktionen, um verschiedene statistische Daten zu versenden, z. B. eine Liste der besuchten Websites, E-Mail-Adressen aus dem Adressbuch des Benutzers oder eine Auflistung von Tastatureingaben.

Die Entwickler von Spyware geben vor, auf diesem Weg die Interessen und Bedürfnisse der Benutzer erkunden zu wollen. Ziel sei es, gezieltere Werbeangebote zu entwickeln. Das Problem dabei ist, dass nicht wirklich zwischen nützlichen und bösartigen Anwendungen unterschieden werden kann. Niemand kann sicher sein, dass die gesammelten Informationen nicht missbraucht werden. Die von Spyware gesammelten Daten enthalten möglicherweise Sicherheitscodes, PINs, Kontonummern usw. Spyware wird oft im Paket mit kostenlosen Versionen eines Programms angeboten, um so Einkünfte zu erzielen oder einen Anreiz für den Erwerb der kommerziellen Version zu schaffen. Oft werden die Benutzer bei der Programminstallation darüber informiert, dass Spyware eingesetzt wird, um sie damit zu einem Upgrade auf die kommerzielle, Spyware-freie Version zu bewegen.

Beispiele für bekannte Freeware-Produkte, die zusammen mit Spyware ausgeliefert werden, sind Client-Anwendungen für P2P-Netzwerke. Programme wie Spyfalcon oder Spy Sheriff gehören zur einer besonderen Kategorie von Spyware: Getarnt als Spyware-Schutzprogramme üben sie selbst Spyware-Funktionen aus.

Wenn auf Ihrem Computer eine Datei als Spyware identifiziert wird, sollte diese gelöscht werden, da sie mit hoher Wahrscheinlichkeit Schadcode enthält.

#### 15.1.7 Potenziell unsichere Anwendungen

Es gibt zahlreiche seriöse Programme, die die Verwaltung miteinander vernetzter Computer vereinfachen sollen. Wenn sie aber in die falschen Hände geraten, kann mit ihnen Schaden angerichtet werden. Mit ESET Cyber Security Pro können solche Bedrohungen erkannt werden.

Zur Kategorie der „potenziell unsicheren Anwendungen“ zählen Programme, die zwar erwünscht sind, jedoch potenziell gefährliche Funktionen bereitstellen. Dazu zählen beispielsweise Programme für das Fernsteuern von Computern (Remotedesktopverbindung), Programme zum Entschlüsseln von Passwörtern und Keylogger (Programme, die aufzeichnen, welche Tasten vom Benutzer gedrückt werden).

Sollten Sie feststellen, dass auf Ihrem Computer eine potenziell unsichere Anwendung vorhanden ist (die Sie nicht selbst installiert haben), wenden Sie sich an Ihren Netzwerkadministrator oder entfernen die Anwendung.

#### 15.1.8 Evtl. unerwünschte Anwendungen

Eventuell unerwünschte Anwendungen sind nicht unbedingt und absichtlich schädlich, sie können aber die Leistung Ihres Computers negativ beeinflussen. Als Benutzer werden Sie normalerweise vor deren Installation zur Bestätigung aufgefordert. Nach erfolgter Installation ändert sich das Systemverhalten (im Vergleich zum Verhalten vor der Installation). Die gravierendsten Veränderungen sind:

- neue Fenster werden angezeigt,
- versteckte Prozesse werden gestartet,
- Prozessor und Speicher werden stärker belastet als zuvor,
- Suchergebnisse ändern sich,
- die Anwendung kommuniziert mit Servern im Internet.

### 15.2 Arten von Remote-Angriffen

Es gibt viele spezielle Methoden, mit denen Angreifer die Kontrolle über Remote-Systeme erlangen oder deren Betrieb stören können. Diese werden in verschiedene Kategorien unterteilt.

#### 15.2.1 DoS-Angriffe

DoS- bzw. Denial-of-Service-Angriffe zielen darauf ab, Computer- oder Netzwerkressourcen für die eigentlichen Nutzer unzugänglich zu machen. Die Kommunikation zwischen betroffenen Benutzern wird behindert und geht nicht mehr ordnungsgemäß vonstatten. In der Regel müssen Sie einen Computer, der einem DoS-Angriff ausgesetzt ist, neu starten. Nur so ist der ordnungsgemäße Betrieb wiederherzustellen.

In den meisten Fällen sind Webserver betroffen. Ziel solcher Angriffe ist es, die Verfügbarkeit der Webserver für einen bestimmten Zeitraum zu unterbrechen.

#### 15.2.2 DNS Poisoning

Mithilfe von „DNS Poisoning“ können Hacker DNS-Server (Domain Name Server) beliebiger Computer über die Echtheit eingeschleuster Daten täuschen. Die nicht authentischen Daten werden für einige Zeit im Cache gespeichert, sodass Angreifer die DNS-Antworten für IP-Adressen umschreiben können. Dies hat zur Folge, dass Benutzer beim Zugriff auf eine Internet-Website nicht den Inhalt der Website, sondern Computerviren oder Würmer herunterladen.

#### 15.2.3 Portscans

Beim Port Scanning wird ein Netzwerkhost auf offene Computerports untersucht. Ein Portscanner ist eine Software zur Erkennung solcher Ports.

Bei einem Computerport handelt es sich um einen virtuellen Punkt zur Abwicklung von ein- und ausgehenden Daten. Für die Sicherheit spielen Ports eine zentrale Rolle. In einem großen Netzwerk können die von Portscannern gesammelten Informationen dazu beitragen, mögliche Sicherheitslücken ausfindig zu machen. Diese Art der Nutzung ist legitim.

Dennoch wird Port Scanning oft von Hackern missbraucht, um Sicherheitsmechanismen zu unterlaufen. In einem ersten Schritt werden Pakete an jeden Port gesendet. Aus der Art der Rückmeldung lässt sich ableiten, welche Ports verwendet werden. Der Portscan selbst verursacht keinen Schaden. Allerdings muss man sich bewusst sein, dass auf diese Weise Sicherheitslücken aufgedeckt werden können und Angreifer dadurch die Möglichkeit haben, die Kontrolle über Remotecomputer zu übernehmen.

Netzwerkadministratoren wird geraten, alle inaktiven Ports zu sperren und alle aktiven Ports vor unerlaubtem Zugriff zu schützen.

#### 15.2.4 TCP Desynchronisation

TCP Desynchronisation ist eine Methode, die bei TCP-Hijacking-Angriffen verwendet wird. Sie wird von einem Prozess ausgelöst, bei dem die Sequenznummer von eingehenden Paketen von der erwarteten Sequenznummer abweicht. Pakete mit einer unerwarteten Sequenznummer werden abgewiesen (oder im Zwischenspeicher abgelegt, wenn sie im aktuellen Kommunikationsfenster enthalten

sind).

Bei der Desynchronisation lehnen beide Kommunikationsendpunkte empfangene Pakete ab. An diesem Punkt können externe Angreifer in das System eindringen und Pakete mit einer korrekten Sequenznummer einschleusen. Die Angreifer können sogar die Daten manipulieren oder verändern.

TCP-Hijacking-Angriffe zielen darauf ab, die Server-Client-Verbindung oder die Peer-to-Peer-Kommunikation zu stören bzw. zu unterbrechen. Viele Angriffe lassen sich durch die Authentifizierung jedes TCP-Segments verhindern. Darüber hinaus ist es ratsam, die empfohlenen Konfigurationen für Ihre Netzwerkgeräte zu verwenden.

#### 15.2.5 SMB Relay

SMBRelay und SMBRelay2 sind spezielle Programme, die in der Lage sind, Angriffe auf Remotecomputer auszuführen. Die Programme nutzen das SMB-Protokoll (Server Message Block), das auf NetBIOS aufbaut, für den gemeinsamen Datenzugriff. Für die Freigabe eines Ordners oder eines Verzeichnisses im LAN wird in der Regel das SMB-Protokoll verwendet.

Im Rahmen der lokalen Netzwerkkommunikation werden Passwort-Hash-Werte ausgetauscht.

SMBRelay empfängt eine Verbindung über die UDP-Ports 139 und 445, leitet die zwischen Client und Server ausgetauschten Pakete weiter und manipuliert sie. Nachdem die Verbindung hergestellt wurde und die Authentifizierung erfolgt ist, wird die Verbindung zum Client getrennt. SMBRelay erstellt eine neue virtuelle IP-Adresse. Bis auf Aushandlungs- und Authentifizierungsdaten leitet SMBRelay alle SMB-Protokolldaten weiter. Angreifer können die IP-Adresse verwenden, solange der Client-Computer verbunden ist.

SMBRelay2 funktioniert nach demselben Prinzip wie SMBRelay, verwendet aber NetBIOS-Namen statt IP-Adressen. Beide können Man-in-the-Middle-Angriffe ausführen. Über diese Art von Angriffen können Angreifer Nachrichten, die zwischen zwei Kommunikationsendpunkten ausgetauscht werden, unbemerkt lesen, einfügen und manipulieren. Computer, die solchen Angriffen ausgesetzt sind, reagieren häufig nicht mehr oder werden ohne ersichtlichen Grund neu gestartet.

Um Angriffe zu vermeiden, sollten Sie Authentifizierungspasswörter oder -schlüssel verwenden.

#### 15.2.6 ICMP-Angriffe

ICMP (Internet Control Message Protocol) ist ein weitverbreitetes Internetprotokoll. Es wird vor allem verwendet, um Fehlermeldungen von vernetzten Computern zu senden.

Angreifer versuchen, die Schwachstellen des ICMP-Protokolls auszunutzen. ICMP wird für einseitige Kommunikation eingesetzt, bei der keine Authentifizierung erforderlich ist. Dadurch können Angreifer sogenannte Denial-of-Service-Angriffe (DoS) starten oder Angriffe ausführen, durch die nicht autorisierte Personen auf eingehende und ausgehende Datenpakete zugreifen können.

Typische Beispiele für ICMP-Angriffe sind Ping-Flood, ICMP_ ECHO-Flood und Smurf-Attacken. Bei einem ICMP-Angriff arbeitet der Computer deutlich langsamer (dies gilt für alle Internetanwendungen), und es treten Probleme mit der Internetverbindung auf.

### 15.3 E-Mail

E-Mail bzw. elektronische Post ist eine moderne Form der Kommunikation, die vielerlei Vorteile bietet. Sie ist flexibel, schnell und direkt und spielte bei der Verbreitung des Internets in den frühen 90er Jahren eine wesentliche Rolle.

Durch die starke Anonymität bieten E-Mails und das Internet leider viel Spielraum für illegale Aktivitäten wie das Versenden von Spam-Mails. Zu Spam zählen unerwünschte Werbung, Hoaxes und die Verbreitung von Schadsoftware - Malware. Die Gefahren und Unannehmlichkeiten werden noch dadurch erhöht, dass das Versenden von Spam nur geringste Kosten verursacht und den Verfassern von Spam viele Tools zum Abgreifen neuer E-Mail-Adressen zur Verfügung stehen. Darüber hinaus erschweren das Ausmaß und die Vielfalt von Spam eine gezielte Bekämpfung des Problems. Je länger Sie Ihre E-Mail-Adresse verwenden, desto wahrscheinlicher ist es, dass sie in einer Spam-Datenbank landet. Nachfolgend finden Sie ein paar Tipps, wie Sie das verhindern können:

- Veröffentlichen Sie möglichst nicht Ihre E-Mail-Adresse im Internet.
- Geben Sie Ihre E-Mail-Adresse nur an vertrauenswürdige Personen weiter.
- Verwenden Sie möglichst keine häufig verwendeten Pseudonyme - bei komplizierteren Pseudonymen ist die Wahrscheinlichkeit der Nachverfolgung geringer.
- Antworten Sie nicht auf Spam-Mails, die sich in Ihrem Posteingang befinden.
- Seien Sie vorsichtig, wenn Sie Internetformulare ausfüllen - achten Sie insbesondere auf Optionen wie *Ja, ich möchte Informationen erhalten.*
- Verwenden Sie separate E-Mail-Adressen - z. B. eine für Ihre Arbeit, eine für die Kommunikation mit Freunden usw.
- Ändern Sie Ihre E-Mail-Adresse von Zeit zu Zeit.
- Verwenden Sie einen Spam-Schutz.

#### 15.3.1 Werbung

Internetwerbung ist eine der am schnellsten wachsenden Werbeformen. Die wesentlichen Vorteile liegen in den geringen Kosten und der direkten Kommunikation; außerdem kommen die Nachrichten beinahe sofort an. Viele Unternehmen nutzen E-Mail-Marketinginstrumente, um effektiv mit ihren bestehenden und potenziellen Neukunden zu kommunizieren.

Diese Art der Werbung ist legitim, da Sie vielleicht Interesse an Werbematerial über manche Produkte haben. Viele Unternehmen senden jedoch unerwünschte Massenwerbung. In diesem Fall überschreitet die Werbung die Grenze des Erlaubten und wird zum Spam.

Die Menge an unerwünschten Werbe-E-Mails ist mittlerweile zu einem enormen Problem geworden und eine Besserung ist nicht in Sicht. Die Verfasser unerwünschter Werbemails versuchen oft, Spam als legitime Nachrichten zu verschleiern.

### 15.3.2 Hoaxes

Ein Hoax ist eine Falschmeldung, die über das Internet verbreitet wird. Hoaxes werden üblicherweise über E-Mail oder Kommunikationsinstrumente wie ICQ oder Skype gesendet. Die Nachricht selbst ist meist ein Scherz oder eine erfundene Geschichte.

Computer-Hoaxes versuchen beim Empfänger Angst, Ungewissheit und Zweifel („fear, uncertainty and doubt", FUD) hervorzurufen, damit dieser glaubt, sein System sei von einem Virus befallen worden, der nicht erkannt wurde und nun Kennwörter abgreift oder anderweitig Schaden am System anrichtet.

Manche Hoaxes fordern den Empfänger auf, die Nachricht an seine Kontakte weiterzuleiten; so wird der Hoax verbreitet und „am Leben erhalten". Es gibt Hoaxes für Handys, Hilfeaufrufe, Menschen, die anbieten, Geld aus dem Ausland zu überweisen usw. Oft ist es unmöglich, die Absicht des Verfassers zu erkennen.

Wenn Sie eine Nachricht erhalten, die Sie an sämtliche Kontakte weiterleiten sollen, dann handelt es sich wahrscheinlich um einen Hoax. Es gibt zahlreiche Internetseiten, auf denen Sie prüfen können, ob eine E-Mail legitim ist oder nicht. Suchen Sie deshalb immer zunächst im Internet nach Informationen über Nachrichten, hinter der Sie einen Hoax vermuten.

### 15.3.3 Phishing

Der Ausdruck Phishing bezeichnet eine kriminelle Vorgehensweise, die mit Social-Engineerung-Techniken arbeitet (Manipulation von Anwendern, um an vertrauliche Daten zu gelangen). Phishing zielt darauf ab, an vertrauliche Daten wie Kontonummern, PIN-Codes usw. zu gelangen.

Die Angreifer erhalten Zugriff, indem sie E-Mails vertrauenswürdiger Personen oder Unternehmen nachahmen (z. B. von Banken oder Versicherungsunternehmen). Solche E-Mails können sehr echt wirken und sogar Grafiken und Inhalte von den Unternehmen enthalten, die sie nachahmen sollen. Sie werden unter einem Vorwand (Datenüberprüfung, Finanztransaktionen) aufgefordert, Ihre persönlichen Daten wie Kontonummern, Benutzernamen oder Kennwörter einzugeben. Wenn Sie diese Daten angeben, können sie mühelos gestohlen oder missbraucht werden.

Banken, Versicherungen und andere seriöse Unternehmen werden Sie nie nach Ihrem Benutzernamen und Kennwort in einer ungebetenen E-Mail fragen.

### 15.3.4 Erkennen von Spam

Es gibt einige Anzeichen, anhand derer Sie Spam (unerwünschte E-Mails) in Ihrem Postfach erkennen können. Wenn eine Nachricht zumindest einige der nachfolgenden Kriterien erfüllt, dann handelt es sich wahrscheinlich um Spam.

- Die Absenderadresse befindet sich nicht in Ihrer Kontaktliste.
- Ihnen wird eine größere Geldsumme in Aussicht gestellt, Sie sollen jedoch zunächst eine kleine Summe zahlen.
- Sie werden unter einem Vorwand (Datenüberprüfung, Finanztransaktionen) aufgefordert, Ihre persönlichen Daten wie Kontonummern, Benutzernamen oder Kennwörter usw. preiszugeben.
- Die Nachricht ist in einer fremden Sprache geschrieben.
- Sie erhalten Werbung für ein Produkt, an dem Sie nicht interessiert sind. Sollten Sie sich dennoch zum Kauf entschließen, überprüfen Sie, dass es sich beim Absender um einen seriösen Händler handelt (ggf. an den Originalhersteller wenden).
- Einige der Wörter enthalten Schreibfehler, um Ihren Spamfilter zu überlisten. Beispiel: *vaigra* anstelle von *viagra* usw.